IT-relaterad brottslighet

BRÅ-rapport 2000:2

Denna rapport kan beställas hos bokhandeln eller hos
Fritzes Kundtjänst, 106 47 Stockholm. Telefon 08-690 91 90,
fax 08-690 91 91, e-post fritzes.order@liber.se

Produktion:
Brottsförebyggande rådet, Information och förlag,
Box 1386, 111 93 Stockholm.Telefon 08-401 87 00, fax 08-411 90 75,
e-post info@brottsforebygganderadet.se
BRÅ på Internet: www.brottsforebygganderadet.se
ISSN 1100-6676, ISBN 91-38-31608-0
Omslag: Ahlm & Partners
Tryck: Tierps Tryckeri AB, Tierp 2000

Innehåll

Förord 5
Sammanfattning 7
Hur har den IT-relaterade brottsligheten utvecklats? 7
BRÅ:s bedömning 9
Inledning 11
Varför en undersökning? 11
Bakgrund 12
Historik 14
Olika typer av IT-relaterade brott 15
Dataintrång 15
Virus och andra ”maliciösa” programvaror 17
Bedrägeri, databedrägeri och svindleri m.m. 17
Utpressning 18
Spel och dobbleri 18
Hot och hets mot folkgrupp 18
Prostitution och barnpornografi 19
Personuppgiftslagen 19
Ungdomsbrottslighet 19
Upphovsrätt 19
Varusmuggling, narkotika och vapen 20
Ekonomisk brottslighet 20
Penningtvätt 20
Organiserad brottslighet 21
Informationskrigföring 21
Resultat 22
Företagsundersökningen 22
Privatpersonsundersökningen 24
Undersökningen av polisanmäld brottslighet 25
De vanligaste brotten 26
Övriga brott 40
Brottsligheten och polisen 42
IT-relaterad brottslighet: Diskussion 45
Gamla brott i nya kläder? 45
Vad betyder den IT-relaterade brottsligheten för oss? Är den allvarlig? 45
Framtiden 47
Slutsatser och förslag 49
Slutsatser 49
Förslag 49
Litteratur 52

Bilagor 55
Bilaga 1 55
Bilaga 2 56
English summary 57

Förord

IT-relaterad brottslighet uppfattas oftast som en ny form av brottslighet. Men så ny är den inte. Redan i början av 1980-talet uppmärksammade Brottsförebyggande rådet (BRÅ) denna brottslighet i en rapport, som var ett av de första vetenskapliga verken som över huvud taget gavs ut på detta område. Det var bland annat genom detta arbete som grunden lades till dagens kunskap om den IT-relaterade brottsligheten.

Många av de tankar som formulerades i BRÅ-rapporten från det tidiga 1980-talet äger ännu giltighet. På en punkt har utvecklingen dock gått åt ett håll som var svårt att förutse. Det gäller Internet. Med den datortäthet och anslutningsgrad till Internet som gäller i den industrialiserade världen, ingår vi alla i det som Marshall McLuhan en gång kallade för *”the global village”*. IT kännetecknas av en extrem rörlighet som inte känner några nationsgränser. På några sekunder kan stora mängder information slussas i nätverken över hela jorden. Därför krävs också internationella lösningar för att bekämpa den IT-relaterade brottsligheten.

Samhället är i dag helt beroende av IT för att kunna fungera. IT har underlättat vår tillvaro inom alla områden samtidigt som samhällets sårbarhet har ökat, inte minst för brott. Den IT-relaterade brottsligheten ska varken underskattas eller överskattas, men hotbilden måste göras tydlig för att relevanta åtgärder ska kunna utarbetas. Dessa förhållanden och den snabba utvecklingen har gjort det nödvändigt att fortsätta kunskapsuppbyggnaden om den IT-relaterade brottsligheten.

Syftet med denna rapport är att ge en bred kunskapsöversikt över IT-relaterad brottslighet. Tonvikten ligger på ett antal undersökningar som genomförts i BRÅ:s regi. Målgrupper är politiker, anställda inom såväl rättsväsendet som andra myndigheter och organisationer som kommer i kontakt med problemet, samt näringslivet och allmänheten.

Författare till rapporten är verksjuristen Lars Emanuelsson Korsell och utredaren Krister Söderman, båda verksamma vid BRÅ. Utredaren Nina Axnäs har svarat för kodningsarbete. Rapporten har granskats av universitetslektorn Louise Yngström vid Institutionen för data- och systemvetenskap (DSV), Stockholms universitet.

Stockholm i januari 2000

Ann-Marie Begler
Generaldirektör

Sammanfattning

Under våren, sommaren och hösten 1999 har BRÅ genomfört en kartläggning av den IT-relaterade brottsligheten i Sverige. De frågor som ställs berör brott, gärningsmän, offer, skador, hotbilder och vilka åtgärder som bör sättas in.

Hur har den IT-relaterade brottsligheten utvecklats?

Sedan år 1995/1996 har de IT-relaterade brotten och incidenterna ökat med 55 procent i företag, myndigheter, kommuner och landsting med fler än 50 anställda (företagsundersökningen). Det betyder att var fjärde organisation har drabbats. Anslutningen till publika nät som Internet har nästan fördubblats under perioden, samtidigt som företagens kontroll- och rapporteringssystem förbättrats.

En trolig förklaring till den kraftiga ökningen är därför en kombination av ökad exponering samtidigt som kontrollsystemen har förbättrats. Annars hade ökningen troligen varit ännu större.

Ökningen av brott och olika incidenter har främst drabbat den privata sektorn. För den offentliga sektorn har ökningen varit väsentligt lägre.

De brott och incidenter som har en framträdande roll i undersökningen är datavirus, externa och interna dataintrång, manipulation av data, stöld av information och bedrägerier.

Datavirus dominerar bland incidenterna i undersökningen. Antalet virusangrepp har ökat med 47 procent sedan mitten av 1990-talet. Datavirus är ett stort eller mycket stort hot mot företagens och myndigheternas verksamheter.

Externa och interna dataintrång är den näst största kategorin efter datavirus. Dataintrången har ökat med 48 procent sedan mitten av 1990-talet enligt företagsundersökningen. Den största ökningen har skett bland företag inom den privata sektorn. För dataintrång är hotet från anställda (insiders) betydligt allvarligare än hotet från utomstående personer (outsiders). Trots detta polisanmäler företagen betydligt fler externa dataintrång än interna (60/40). Skälet kan vara att företagen löser de interna dataintrången själva. Företagen anser också att de kan förlora i anseende om det blir känt att känsliga IT-relaterade brott inträffat. Enligt undersökningen polisanmäldes åren 1997 och 1998, 239 externa och interna dataintrång.

Manipulation av data och *stöld av information* är brottstyper som företagen i dag inte beskriver som särskilt omfattande. Trots detta bör denna typ av brott tas på största allvar eftersom skadorna ofta är stora. Företagens information om produktutveckling, marknadsföring, upphandling, personal etc. representerar mycket stora kommersiella värden.

Manipulation i någon form har ökat med 80 procent och antalet informationsstölder har ökat med 22 procent sedan år 1995. Trots de skador som kan uppkomma är det drygt hälften av de tillfrågade företagen, myndigheterna m.fl. som anser att manipulation och stöld av information är ett mindre hot mot verksamheten. Enligt BRÅ:s bedömningar finns det anledning att ändå ta dessa hot på stort allvar.

Drygt hälften av de undersökta polisanmälningarna inom IT-området är *bedrägerier* via Internet (329). De vanligaste formerna är att utnyttja annans Internetabonnemang (frisurfande) och att köpa på nätet med annans kontokortsnummer. Mellan åren 1997 och 1998 skedde en kraftig ökning av anmälningarna avseende bedrägeri via Internet. Majoriteten av bedrägerierna anmäls av privatpersoner.

Övrig polisanmäld brottslighet är hot och trakasserier (7), skadegörelse (16) och integritetsbrott (17).

Tre av hundra privatpersoner med Internetabonnemang har utsatts för hot eller trakasserier via e-post. Vidare har fem av hundra privatpersoner med Internetabonnemang stött på barnpornografi på nätet och tolv av hundra har sett en nazistisk webbsida.

Gärningsmän

Det är, utifrån BRÅ:s undersökningar, inte lätt att få en bild av gärningsmännen. Den bild som framskymtar är att de flesta brott och incidenter begås av outsiders. Räknar man bort virusangrepp och externa dataintrång, som är vanligast, svarar emellertid insiders för huvuddelen av brotten och incidenterna (63 procent).

Bland den polisanmälda brottsligheten dominerar männen som gärningsmän, endast ett fåtal kvinnor anges som misstänkta gärningsmän. Män misstänks för dataintrång, de manipulerar, raderar och stjäl program, filer eller data. När kvinnor misstänks som gärningsmän handlar det mestadels om interna dataintrång – obehörig registerupplysning och radering av filer, program eller data. Endast tre kvinnor misstänks för databedrägeri. Sammanlagt finns det tio misstänkta kvinnor av totalt 116 misstänkta gärningsmän bland polisanmälningarna. Omkring 68 procent av de misstänkta gärningsmännen är i åldern 15 till 25 år.

Säkerhet och skador

Säkerheten har ökat markant under senare år. Exempelvis har andelen företag som har förebyggande skydd mot externa dataintrång ökat från 40 till drygt 65 procent på bara några år. Den privata sektorn är sämre än den offentliga sektorn på att förebygga externa dataintrång.

Knappt hälften av alla företag har rutiner för att förebygga manipulation av något slag för hela verksamheten. De offentliga verksamheterna är bättre rustade än de privata i detta avseende. Nästan hälften av samtliga företag, myndigheter, kommuner och landsting saknar rutiner för att rapportera stöld av information.

De skattade sammanlagda skadorna för IT-relaterade brott och incidenter uppgår till mellan 37,5 och 238,6 miljoner kronor. Den genomsnittliga kostnaden under ett år för de företag som drabbas är cirka 140 000 kronor.

Rättsväsendet

De flesta företag som BRÅ har intervjuat anser att de har ett bra samarbete med myndigheter. Samtidigt anser de att myndigheterna saknar förmåga att utreda och lagföra IT-relaterad brottslighet.

Av privatpersoner med Internetabonnemang anser endast ett fåtal att polisens resurser är tillräckliga när det gäller brottslighet på Internet. Genomgående anser man att polisen behöver mer resurser. Å andra sidan uppger nästan hälften av samma grupp att brottsligheten på Internet är alltifrån liten till obefintlig.

BRÅ:s bedömning

IT-utvecklingen och globaliseringen innebär omvälvande förändringar av samhället och nya tillfällen till brott. Förutsättningar skapas för mycket allvarliga brott. Men det behöver inte betyda att sådana brott kommer att ske i den omfattning som det finns tekniska förutsättningar för. En kombination av ytterligare faktorer krävs, bland annat hög teknisk kompetens, mycket stark motivation för att begå brottet och tillgång till insiders. Därtill kommer att en utveckling också sker på det brottsförebyggande och brottsbekämpande området. Hur alla dessa faktorer kan komma att kombineras går inte att svara på, men facit behöver inte bli den dramatiska brottslighet som ibland förespeglas.

Rapporten gör inte anspråk på att beskriva hela den IT-relaterade brottsligheten eftersom den täcker ett mycket stort område av olika brottstyper. De undersökningar som BRÅ genomfört ger dock inte bilden av att det förekommer en IT-relaterad brottslighet med sådana dramatiska förtecken som den mytologiserade bild man gärna skapar av den. De flesta IT-relaterade brott är snarare av ”vardagskaraktär”, det vill säga det är frågan om traditionella brott. Ett par allvarligare IT-relaterade brott har dock kommit fram i BRÅ:s undersökningar, bland annat stöld av information. Säkerheten mot stöld och manipulation av information visar sig vara bristfällig.

BRÅ anser att framför allt näringslivet måste satsa på förebyggande åtgärder för att skydda känslig information. Även medvetenheten om farorna med manipulation av information bör öka.

Förebyggande arbete på företag, banker, myndigheter och hos privatpersoner är det effektivaste sättet att skydda sig mot olika typer av brott. I IT-samhället kommer det förebyggande arbetet att vara än viktigare, eftersom den IT-relaterade brottsligheten verkar globalt och är svår att utreda och lagföra.

IT-relaterade brott handlar till stor del om tekniska och organisatoriska brister. De förebyggande lösningarna måste därför i hög grad vara av teknisk och administrativ art. Men IT-säkerhet kan inte enbart kretsa kring tekniska åtgärder som brandväggar, behörighetsnivåer, lösenord m.m. Eftersom insiderhotet är störst måste man också främja en öppen dialog på arbetsplatser och därigenom skapa förutsättningar för interna organisatoriska lösningar. Sådana åtgärder är också viktiga inslag i säkerhetstänkandet.

Det är högst sannolikt att allt fler brott i framtiden kommer att vara IT-relaterade. Därför måste rättsväsendet i större utsträckning kunna hantera sådana ärenden och mål. Tydligt är också att det finns behov av särskild spetskompetens. Men på sikt minskar behovet av att särskilja IT-relaterade brott från andra brott.

Ansvaret för IT-säkerheten bör tydliggöras, exempelvis genom att en myndighet tilldelas huvudansvaret. Det handlar om att samordna olika aktörer, sprida information om förebyggande åtgärder etc.

Spaning på nätet är ett instrument för kontrollmyndigheterna att förebygga och upptäcka brott. Kontrollmyndigheternas och de brottsbekämpande myndigheternas underrättelsetjänstsverksamhet behöver stärkas.

Internationellt samarbete är en förutsättning för en effektiv bekämpning av en brottslighet som utförs med en teknik som inte känner några nationsgränser.

Inledning

Varför en undersökning?

Den IT-relaterade brottsligheten är mytomspunnen (SOU 1992:110). Det engelska uttrycket *”cybercrime*” eller franska *”criminalité informatique”* för tanken till en framtida brottslighet av närmast science fiction-karaktär. Historier sprids om smarta ungdomar som nästlat sig in i Pentagons datorer eller om den organiserade brottsligheten i Ryssland som fört över miljardbelopp mellan bankkonton genom att gå in i nätverken. Den fråga som ställs här är därför: Vad handlar den IT-relaterade brottsligheten egentligen om och hur ser den ut i Sverige?

Den IT-relaterade brottsligheten är inte någon homogen brottskategori utan spänner över ett stort antal brottstyper från bedrägerier till spridning av barnpornografi. Det är därför inte möjligt att presentera en enhetlig framställning av brottsligheten. För att få ett så brett perspektiv på brottsligheten som möjligt har olika undersökningsmetoder använts, riktade mot olika målgrupper. Utöver en litteraturgenomgång har följande empiriska undersökningar genomförts. Undersökningarna har genomförts under våren, sommaren och hösten 1999.

- Brevenkät (företagsundersökningen) till 1 564 företag, statliga myndigheter och bolag, kommunal förvaltning och bolag samt landsting med minst 50 anställda (1 007 har svarat, 67 procent[1]). Företagsundersökningen är en upprepning av en undersökning Riksrevisionsverket (RRV) genomförde år 1997 och som avsåg IT-relaterade brott och incidenter under åren 1995-1996. BRÅ:s undersökning avser åren 1997-1998.
- Telefonintervjuer (privatpersonsundersökningen) med 1 000 privatpersoner med Internetabonnemang. Frågorna berörde dataintrång, datavirus och hur man upplevde säkerheten vid näthandel, brottsligheten på Internet och polisens resurser för att bekämpa brottsligheten.
- Genomgång av samtliga polisanmälningar (undersökningen av polisanmäld brottslighet) under åren 1997 och 1998, kodade som dataintrång, datasabotage, datortidsstöld, trolöshet mot huvudman angående datorteknik, datorbedrägeri och integritetsskyddsbrott (totalt 608 anmälningar efter rensning av felkodningar etc.).
- Intervjuer (intervjuundersökningen) med omkring 30 IT-chefer, säkerhetsansvariga, experter m.fl. Intervjupersonerna ombads beskriva hotbilder, redogöra för incidenter inom företagen och för problem med IT-säkerhet och eventuella brott. Intervjupersonerna är anonyma.

---

[1] Svarsfrekvensen kan anses som god med tanke på ämnets känslighet. I andra liknande enkätundersökningar har svarsfrekvenserna legat omkring 20-40 procent, med undantag för RRV:s enkät som uppnådde 77 procent.

Bakgrund

Kort om begreppet IT-relaterad brottslighet

IT-relaterad brottslighet är vad man inom kriminologin kallar för modern brottslighet. Här menas en brottslighet som uppstått bland annat på grund av den tekniska utvecklingen eller ny lagstiftning (Alalehto, 1999). Begreppet IT-relaterad brottslighet är ett samlingsbegrepp på brottslighet som har med datorteknik att göra. Själva begreppet finns inte i lagstiftningen och de brott som avses faller in under en mängd olika straffbestämmelser som är teknikneutrala, dvs. de behandlar skadegörelse, olaga hot m.m. oavsett om det sker med IT eller inte. Det finns ändå några straffbestämmelser som särskilt tar sikte på IT – databedrägeri och dataintrång.

I denna rapport används begreppet IT-relaterad brottslighet. Tidigare talades det om databrott. Databrott, datorbrott och datorrelaterad brottslighet är samlingsbenämningar på sådana straffbara gärningar som på ett eller annat sätt anknyter till ADB, telekommunikation och annan modern informationsteknologi (Seipel, 1990). Definitionen av IT varierar, ibland avses enbart datorrelaterad teknik och ibland även telekommunikation och till och med hemelektronik (Ibid). I denna rapport avses med IT i huvudsak datorrelaterad teknik.

Den IT-relaterade brottsligheten sker i datamiljö eller med hjälp av datorteknik i åtminstone en av följande tre situationer (Savona, 1998):

1. Datorn (informationsbäraren) kan vara *målet* för brottet. Gärningsmannens syfte är exempelvis att stjäla eller förstöra information genom att göra ett intrång i en dator.
2. Datortekniken kan var ett *medel* för att begå brottet. Gärningsmannen använder datorn som ett verktyg för att begå brottet.
3. Datorn kan, utan att vara mål eller medel, ha *beröring* med brottet. En dator kan exempelvis användas för att registrera narkotikaleveranser. Datorn kan härigenom ha betydelse för brottsutredningen[2].

Samhällets förändring och brottsligheten

Utvecklingen går snabbt. För inte så många år sedan fylldes industrierna av arbetskraft från de gamla basnäringarna jord- och skogsbruk. Nu minskar sysselsättningen i tillverkningsindustrin; arbetskraften flyttar in bakom service- och informationssamhällets dataskärmar. Traktorerna ersatte en gång hästarna,

[2] När det gäller punkten tre är det inte självklart hur nära anknytning till datorteknik ett brott måste ha för att det ska vara IT-relaterat. Malmsten (1979:250) menar att det gäller brottsliga gärningar som har en ”inte alltför avlägsen anknytning” till datorer.

nu upplever många att maskiner och datorer tar över arbetet från stora grupper av människor (Magnusson, 1996). I dag kretsar utvecklingen kring globaliseringen och informationstekniken.

Liksom industrialismen och inflyttningen till städerna innebar förändringar av brottsligheten och andra sociala mönster, har globaliseringen och IT påverkat våra livsmönster och utvecklingen på det kriminella området. Sannolikt har vi bara sett början på en fortsatt utveckling av snabba och omfattande strukturella förändringar (Castells, 1996).

IT inte enbart ”connecting people”

Den internationella diskussionen om det aktuella hotet från brottsligheten gäller terrorism och organiserad brottslighet (Falletti, 1998). Den organiserade brottsligheten är involverad i narkotika, utpressning, stölder, vapenhandel, människosmuggling och korruption samt handel med kvinnor och barn. Som nya måltavlor för brottsligheten anges IT och Internet. För den organiserade brottsligheten har Internet betraktats som ”en gåva från himlen” (Ziegler, 1998:240). Även i Sverige har som en internationell trend, globaliseringen, datoriseringen och den organiserade brottsligheten lyfts fram (Internationella ekobrottsgruppen, 1997). Enligt Castells (1998) kommer kriminella nätverk att utgöra en betydelsefull del av ekonomin, samhällets institutioner och vardagsliv. Kriminella aktiviteter över hela världen kan gå samman och bilda en global kriminell ekonomi som penetrerar finansmarknader, handel, företag och politiska system i alla samhällen. Castells pekar också på terroristhotet. Ökad sofistikerad teknik medför att en liten beslutsam grupp, som är välfinansierad och välinformerad, kan ödelägga hela städer eller slå till mot vitala punkter i samhället.

I takt med IT-utvecklingen kommer givetvis fler brott att vara IT-relaterade (Solarz, 1985 och Sieber, 1998). I och med att kunnandet om tekniken ökar i allt bredare kretsar, finns en risk för allvarligare brott. En särskild fara är om datakunnandet sprids till yrkeskriminella som överger traditionella former för brott och i stället övergår till IT-relaterad brottslighet (NCIS, 1999).

När bilen började rulla på våra vägar blev även brottslingen mobil och brotten kunde utföras på ett större geografiskt område än tidigare. På samma sätt inverkar IT inte enbart på brottsligheten indirekt via genomgripande strukturella förändringar av samhället, utan också på ett direkt plan. IT befriar oss från ”rummets tyranni” (Davidson och Rees-Mogg, 1997). Utan tidigare motstycke har IT skapat förutsättningar för att etablera en verksamhet och utföra ett arbete praktiskt taget var som helst på jorden. Ett intrång i en svensk dator kan ske från ett annat land eftersom datorerna är kopplade till varandra genom nätverken. Från vilken plats som helst kan förbjudna varor bjudas ut till försäljning på nätet. Pengar från brottslig verksamhet kan blixtsnabbt överföras till banker på andra sidan jordklotet.

Utvecklingen går nu mot mer användarvänlig teknik, vilket ökar riskerna för att fler personer med brottsliga avsikter kan utnyttja tekniken. Bäst beskrivs

detta av en intervjuperson inom polisen*: ”…för några år sedan var en hacker tvungen att kunna Unix utan och innan. I dag kan man ladda hem ett program från Internet som gör samma sak. Jag brukar kalla det för Plug and Play hacking”*.

Datoranvändarens anonymitet och avsaknaden av den fysiska närvaron av brottet och dess konsekvenser, skapar förutsättningar för att begå brott på nätet som gärningsmannen aldrig skulle ha drömt om att göra i ”den gamla vanliga världen” (Rasch, 1996). *”Med den nya informationsteknologin uppstår tillfällen till brott i en utsträckning och storlek utan tidigare motstycke.”* (Grabosky, Smith och Wright, 1998:13). Sådana brott kännetecknas av overklighet och av att det inte finns något tydligt offer (Mann och Sutton, 1998). De normer och värderingar som sätter gränser för vårt beteende i den verkliga världen gäller inte lika självklart i IT-miljön.

Historik

Uppmärksamheten kring den IT-relaterade brottsligheten har ökat parallellt med den tekniska utvecklingen och ökad användning av IT. Men de hot som man diskuterat har också förändrats i takt med att ny teknik har utvecklats.

Under mitten av 1980-talet handlade IT-relaterad brottslighet mest om förskingring utförd av insiders. Det var stordatorernas tid och säkerheten kring dessa var i fokus. Under slutet av 1980-talet växte nätverken upp och hackern fick stor uppmärksamhet i medierna. Det var en tid av demonisering eller romantisering av hackern (Hallinger, 1997). Stordatorerna byttes ut mot PC:n och IT fick en större spridning. I början av 1990-talet konstaterade Datastraffrättsutredningen att undersökningar inte tydde på någon stor databrottslighet (SOU 1992:110). Utredningen antog emellertid att olovlig kopiering av programvara, dataintrång och virus förekom i ett stort antal fall. I dag kretsar frågorna om information och det stora värde som ligger i information och andra immateriella tillgångar (Martin, 1997). Dessutom handlar diskussionen om Internet och elektronisk handel.

Olika typer av IT-relaterade brott

I det följande beskrivs olika brott och incidenter som är eller kan vara IT-relaterade. Här redovisas både olika brottstyper, exempelvis dataintrång och bedrägerier, och mer övergripande fenomen, exempelvis ekonomisk brottslighet och ungdomsbrottslighet, som egentligen är samlingsbeteckningar på brottstyper med särskilda kännetecken. Vissa överlappningar kommer därför att ske.

På det straffrättsliga området pågår en diskussion om hur mycket lagstiftningen måste ändras för att anpassas till IT.[3]

Dataintrång

Det är brottsligt att olovligen ta sig in i ett datasystem, så kallat dataintrång (4 kap. 9 c § brottsbalken). Bestämmelsen täcker sådana gärningar som man brukar tillskriva hackers och crackers.

En hacker är en dataintresserad person som olovligen tar sig in i ett datasystem för att undersöka och utforska det. Syftet är inte att förstöra, stjäla eller förändra information (Parker, 1998). En cracker gör också dataintrång, men har andra syften än hackern, till exempel att förstöra, kopiera eller ändra information. Inom crackergruppen finns de största externa hoten för företag och andra organisationer. Stöld av företagshemlig information och sabotage av strategiska datasystem, program eller data kan vara angreppsobjekt för en cracker.

Crackerns brott bedöms också som dataintrång, men andra brott kan ta över beroende på gärningens art, till exempel bedrägeri, skadegörelse, sabotage, brott enligt upphovsrättslagen eller brott enligt lagen (1990:409) om skydd av företagshemligheter. I kriminologisk mening kan därför dataintrång i realiteten vara en samlingsbeteckning på olika brott, som har det gemensamt att det är nödvändigt att göra intrång i datasystem för att utföra gärningarna. Dataintrånget kan vara själva målet (hackern), men också medlet för gärningarna (crackern).

[3] Något förenklat utgörs falangerna av vissa som anser att det krävs relativt omfattande förändringar till följd av IT:s karaktäristika, medan andra i huvudsak anser att dagens teknikneutrala lagstiftning också står sig i IT-samhället (SOU 1992:110, PM 1997, 1998 och 1999).

När det gäller brottet företagsspionerи enligt lagen om skydd av företagshemligheter, finns en enda brottmålsdom meddelad[4]. En ung person hade genom externt intrång tagit sig in i en dator och till sin egen dator överfört en stor mängd företagshemligheter. Ingenting tyder på att syftet var att använda företagshemligheter på något allvarligt sätt. Påföljden blev också enbart villkorlig dom och dagsböter.

Med interna dataintrång avses att någon inom företaget eller organisationen (insider) olovligen bereder sig tillgång till data, filer eller program.

Motiven för dataintrånget varierar beroende på vem som är gärningsman. Det förekommer dataintrång som utgör hämnd från före detta anställda, men också stöld av information[5], bedrägerier, förskingring eller trolöshet mot huvudman med motivet att tillskansa sig pengar.

År 1999 genomförde CSI/FBI[6] en undersökning av amerikanska företag och organisationer som visade att enbart 32 procent av de tillfrågade, som hade blivit utsatta för ett dataintrång, hade anmält händelsen till myndigheterna (CSI, 1999). Enligt samma undersökning hade 55 procent av de tillfrågade varit utsatta för dataintrång från anställda och 30 procent från någon utanför. Enligt den brittiska underrättelsetjänsten redovisas lägre siffror i Storbritannien (NCIS, 1999).

Den dolda brottsligheten kan bedömas som stor eftersom det finns flera skäl till varför denna typ av brott inte anmäls. Företaget kan exempelvis anse att det kan skapa negativ publicitet om brottet blir allmänt känt och därmed ytterligare skador, eller som en säkerhetschef uttryckte saken: *”Det är dyrt med dataintrång. Kommer det ut blir det ännu dyrare”*. Dataintrånget kanske inte heller upptäcks. Försvarsdepartementet i USA gjorde, i syfte att testa säkerheten, intrång i 3 000 av Pentagons datorer. Enbart fem procent av användarna hade upptäckt intrånget (Martin, 1997).

Industrispionage syftar till att komma över information som är värdefull för konkurrenter. Det kan handla om teknisk information och produktutveckling, men också om affärskoncept, marknadsföringsstrategier, kundregister etc. IT har skapat nya förutsättningar för spionage genom dataintrång. Spionaget kan också ha militära och säkerhetspolitiska syften.

Ett relativt nytt fenomen, som dykt upp under de senaste åren, är dataintrång som tar sikte på att ändra webbsidor. Syftet kan vara att förmedla ideologiska budskap. Det förekommer att gärningsmannen går in på webbplatser och ändrar länkar så att de hänvisar till webbsidor som innehåller pornografi, nazistisk propaganda etc. Kända fall var när det brittiska Labour Party år 1996 fick en länk på sin webbplats till ”Labour Party Sex Shop” eller när CIA:s webbplats samma år ändrades till ”Criminal Stupidity Agency” (NCIS, 1999).

---

[4] Skadeståndsfrågor enligt denna lag har meddelats av Arbetsdomstolen och Högsta domstolen, AD 80/1998 och HD T1038/97.

[5] I denna rapport används begreppet stöld av information i kriminologisk och inte straffrättslig mening. Straffrättsligt rubriceras stöld av information som till exempel brott mot upphovsrättslagen eller företagsspionerи, eventuellt även som dataintrång.

[6] Computer Security Institute (CSI) och Federal Bureau of Investigation (FBI).

I år har dataintrång bland annat skett på den amerikanska arméns webbplats och även på FBI:s. På den senare hade följande text lagts in: ”Vem skrattar sist?” (Alberganti, 1999). Ett svenskt exempel är när telefonföretaget Telia fick se sitt namn på webbplatsen ändrat till ”Felia”.

Virus och andra ”maliciösa” programvaror

Den vanligaste formen av datorrelaterade incidenter är virus; uttrycket incident används eftersom virusangrepp vanligtvis inte är brottsliga. För att brott ska föreligga krävs enligt svensk lag uppsåt (4 kap. 9 c § brottsbalken, dataintrång). Datastraffrättsutredningen föreslog emellertid i början av 1990-talet att framställning eller spridning av skadegörande virus skulle kriminaliseras (SOU 1992:110), men förslaget har inte lett till lagstiftning. Eftersom det är fråga om beteenden som ofta är på gränsen till det straffbara, ingår virus i BRÅ:s undersökning.

Genom utvecklingen av nätverk och e-post sprids numera virus och andra ”maliciösa” program i en skala som tidigare inte varit möjlig. Detta har lett till att virus numera ses som ett hot av strategisk natur för företag och andra organisationer. Att det är fråga om ett hot framgår tydligt av BRÅ:s undersökningar.

Bedrägeri, databedrägeri och svindleri m.m.

Internet har skapat ett globalt marknadstorg för marknadsföring och försäljning. Samtidigt har det blivit möjligt att vilseleda enskilda och företag att köpa varor och tjänster som inte håller vad de lovar eller att göra investeringar i projekt som saknar verklighetsbakgrund. På Internet kan man också utföra bedrägerier genom att använda någon annan persons kreditkort som stulits eller kreditkortsnummer som gärningsmannen kommit över. Falsk information kan användas i ett svindleri för att manipulera börskurser. Kort och datachips kan förfalskas för att ta ut andras pengar.

Den som ändrar i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling så att det innebär vinning för gärningsmannen och skada för någon annan, kan dömas till bedrägeri (9 kap. 1 § andra stycket brottsbalken). Denna form av bedrägeribrott benämns också databedrägeri.

I takt med användningen av Internet har bedrägerierna ökat (NCIS, 1999). Det gäller investeringsbedrägerier, varor och tjänster som inte existerar etc. I USA skickades falsk information ut på nätet om ett företagsförvärv, vilket medförde att aktiekursen steg med 30 procent. Ett annat fall gällde försäljning av aktier i företag som inte existerade (NCIS, 1999). Internet medför ett kraftigt genomslag för bedrägerier och svindlerier eftersom nätet är globalt. Utan

större kostnader kan gärningsmannen vända sig till ett oräkneligt antal potentiella offer.

Utpressning

Utpressning sker när gärningsmannen genom olaga tvång förmår någon till handling eller underlåtenhet som innebär vinning för gärningsmannen och skada för den tvungne (9 kap. 4 § brottsbalken). Utpressning är en klassisk inkomstkälla för den organiserade brottsligheten på kontinenten (Matard-Bonucci, 1994).

Genom dataintrång eller på annat sätt kan gärningsmannen komma över värdefull information, som sedan kan användas i utpressningssyfte. Under 1998 utsattes Verbraucherbank i Tyskland för utpressning. Gärningsmannen begärde en miljon DM i utbyte mot bland annat information om bankkunder (NCIS, 1999).

Spel och dobbleri

Internet fungerar som en global mötesplats för spelare. Illegal spelverksamhet (dobbleri) kan således bedrivas på nätet (16 kap. 14 § brottsbalken).

År 1998 fanns det mer än 1 000 webbplatser med spelverksamhet. Vissa spel är olagliga, andra kan utnyttjas i bedrägligt syfte. En tendens är att spelverksamhet bedrivs från stater med liten kontroll. År 1998 fanns det 160 virtuella kasinon; 70 procent var baserade i Karibien (NCIS, 1999). Spelsidorna erbjuder traditionella spel som poker och black-jack, japanerna kan satsa pengar i tävlingar med sumobrottare och australiensarna i fotboll etc. (Martin, 1997).

Hot och hets mot folkgrupp

Via Internet sprids rasistisk propaganda, vilket kan bedömas som hets mot folkgrupp (16 kap. 8 § brottsbalken). Därmed aktualiseras också frågan om hur långt yttrandefriheten når. Även annan hatpropaganda kan spridas. I början av år 1999 fanns det omkring 40 webbplatser med nazistiskt eller rasideologiskt budskap i Sverige (Taloyan, 1999).

I USA innehöll en webbplats mot aborter en ”hitlist” med flera hundra namn på läkare som utförde aborter (NCIS, 1999).

Med e-post kan någon hota en annan person (olaga hot, 4 kap. 5 § brottsbalken).

Prostitution och barnpornografi

På Internet kan kunder komma i kontakt med prostituerade. Sådan verksamhet kan i vissa situationer avse brottet koppleri (6 kap. 8 § brottsbalken). Köp av sexuella tjänster är numera straffbart (lagen [1998:408] om förbud mot köp av sexuella tjänster). Enligt Rikskriminalpolisen förmedlas sexuella tjänster i allt högre grad via Internet. Bedömningen är också att det finns risk för att den Internetbaserade prostitutionen och koppleriverksamheten kommer att öka. På nätet finns kontaktannonser, som är täckmantel för försäljning av sexuella tjänster, och webbplatser med annonser om eskortservice. Via Internet sprids också barnpornografiska bilder, vilket räknas som barnpornografibrott (16 kap. 10 a § brottsbalken).

Personuppgiftslagen

Syftet med personuppgiftslagen (1998:204), som ersatt datalagen, är att skydda människors personliga integritet vid behandling av personuppgifter. Lagen, som innehåller straffrättsliga sanktioner, reglerar under vilka förutsättningar personuppgifter får behandlas.

Ungdomsbrottslighet

I en undersökning av hur ungdomsbrottsligheten förändrats sedan början av 1970-talet pekas på att nya brottstyper kan ha tillkommit, som begås av i övrigt skötsamma ungdomar (Ward, 1998). Enligt undersökningen har möjligheterna att begå brott ökat i samband med mer abstrakta kommunikationsformer som personliga koder, datorer och personnummer. Det är också sådana brott som ”en i övrigt laglydig pojke kan tänkas ägna sig åt då dessa brott ofta förknippas med smarthet och datakunnande” (Ward, 1998:50). Omfattningen av detta problem är ännu inte känt.

Upphovsrätt

Enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk har den som skapat ett litterärt eller konstnärligt verk upphovsrätt till detta. Med sådant verk avses exempelvis datorprogram och musikaliska verk. Tekniken gör det i dag möjligt att utan dyrbar utrustning kopiera och sprida program, spel, musik etc. För enskilt bruk får enstaka exemplar av ett verk kopieras (gäller ej datorprogram). Piratkopiering förekommer i stor omfattning av framför allt dataprogram och musik-CD, vilket innebär stora förluster för enskilda

och företag. Överträdelser av upphovsrätten regleras av både civilrättsliga och straffrättsliga bestämmelser.

Ett tecken på omfattningen av piratutgivning är uppgifter om att enbart 0,5 dataprogram sålts per PC (Sieber, 1998). Enligt en undersökning var 31 procent av de mjukvaror som företag i Storbritannien använde under år 1997 olagligt kopierade (NCIS, 1999). Enligt FBI är försäljningen av piratkopior ett internationellt problem med inslag av organiserade brottslingar (NCIS, 1999).

Varusmuggling, narkotika och vapen

Via Internet kan handel ske med förbjudna varor eller som ett led för skatteundandragande. Det kan handla om allt från narkotika, sprit och tobak till skyddade djur och ägg.

Relevant lagstiftning är bland annat lagen (1960:418) om straff för varusmuggling och narkotikastrafflagen (1968:64). På Internet kan också information spridas om hur man begår brott, till exempel hur man kan se på satellit-TV utan att betala avgift eller hur man öppnar lås (Mann och Sutton, 1998).

Ekonomisk brottslighet

”Finns det inte en dator med i bilden är det inte något ekobrott” säger en polisman med lång erfarenhet av ekobrottsutredningar.

Eftersom bokföring, administration och kapitalförvaltning som regel är datoriserad, är sannolikt de flesta ekobrott IT-relaterade. IT används för att tillverka falska handlingar, till exempel registreringsbevis för bolag eller fakturor, som ett led i ekonomisk brottslighet.

IT-utvecklingen har ökat möjligheterna att undandra skattemedel genom olika fiktiva transaktioner över nätet med företag som är stationerade i skatteparadis. För skattekontrollen innebär IT, Internethandel och möjligheten att bedriva verksamhet på nätet svårigheter (Westberg, 1998).

Penningtvätt

Penningtvätt går ut på att förvandla svarta pengar till vita (SOU 1997:36). Enligt lagen (1993:768) om åtgärder mot penningtvätt ska banker och andra institutioner, som hanterar medel, granska alla transaktioner som skäligen kan antas utgöra penningtvätt. Penningtvätt kan bestraffas som penninghäleri eller penninghäleriförseelse enligt 9 kap. 6 a och 7 a § brottsbalken.

Globaliseringen av ekonomin, integrationen av de finansiella marknaderna, nya finansiella tjänster och den kraftiga ökningen av Internet, som medel för finansiella överföringar, har ökat förutsättningarna för penningtvätt (Savona,

1998). Eftersom penningströmmar över nätet kan föras mellan olika länder försvåras myndigheternas kontroll.

Finanspolisen har under de senaste åren tagit emot omkring 1 000 penningtvättsanmälningar om året. Tendensen sedan år 1996 är att anmälningarna ökar. I de ärenden som Finanspolisen ser förekommer dock inte några överföringar av medel på Internet.

Organiserad brottslighet

Enligt Finanspolisen finns det ännu inga tydliga tecken på att den organiserade brottsligheten i Sverige har börjat använda Internet som brottsarena eller tagit till sig den senaste tekniken för dataintrång. Men man uppger att det finns tecken på att Internet och andra IT-strukturer i ökande grad används av den organiserade brottsligheten, till exempel e-post, SMS-meddelanden och chatkanaler för kommunikation och ledning. I en rapport varnar Rikskriminalpolisen för att den organiserade brottsligheten lyckas knyta olika typer av IT-experter, inte minst insiders, till nya typer av brottsupplägg som är svåra att upptäcka och utreda.

Även enligt den brittiska underrättelsetjänsten finns det få belägg för att dataintrång utförts av yrkeskriminella (NCIS, 1999). Men den organiserade brottsligheten använder sig av Internet som kommunikationsmedel med krypterade meddelanden (Ziegler, 1998). Det kan gälla narkotikatrafik, spel, prostitution, vapenhandel etc. (Grabosky, 1998). Enligt Rikskriminalpolisen är kryptering ännu inte rutin i den svenska kriminella kommunikationen via Internet.

Informationskrigföring

IT-beroendet och sårbarheten kan utgöra ett säkerhetspolitiskt hot. Informationskrigföring är en realitet vid sidan av det konventionella sättet att föra krig. Det handlar om att skydda de egna datorsystemen mot angrepp, men också om att angripa motståndaren för att komma över, manipulera eller förstöra värdefull information (Ag IW, 1997 och 1998). Svenska försvaret har kompetens att göra dataintrång, uppger en underrättelseofficer. Under kriget i Bosnien drabbades Sverige när en grupp slog ut flera kommunikationssatelliter för teletrafik. Den nya tekniken kan åstadkomma ett elektroniskt Pearl Harbour varför det över hela världen satsas stora belopp på informationskrigföring (Grabosky, 1998).

Resultat

Först redovisas de generella dragen i BRÅ:s undersökningar med en bild av brottsligheten och förändringar under senare delen av 1990-talet. Därefter redovisas respektive brottskategori var för sig.

Företagsundersökningen

Av företag, myndigheter, kommuner och landsting (fortsättningsvis kallade företag) med minst 50 anställda har 24 procent drabbats av en eller flera incidenter. Det är en fördubbling av antalet företag som rapporterat incidenter i jämförelse med RRV:s enkät för åren 1995-1996. BRÅ har skattat antalet företag med mer än 50 anställda som drabbats till 1 175.

Tabell 1. Skattat antal rapporterade IT-relaterade brott och incidenter, åren 1997-1998. Samtliga brott och incidenter indelade i respektive gärningstypologi och i jämförelse med RRV:s undersökning åren 1995-1996.

Brott	RRV	BRÅ
Datavirus	530	778
Dataintrång (hacking)	117	173
Dataintrång/Datavirus	--	70
Manipulation[7]	76	137
Olovligt utnyttjande av skyddsvärd ADB-lagrad information	27	25
Stöld/olovlig kopiering av ADB-lagrad information med väsentligt värde eller icke standardprogramvara	40	49
Summa	790	1 232

Datavirus är det mest rapporterade brottet/incidenten, därefter kommer dataintrång. Av tabell 1 framgår att virus och hacking ökat med 47 respektive 48 procent[8]. Manipulation har ökat med 78 procent. Datavirus och dataintrång sammantaget står för 83 procent av samtliga brott och incidenter och dessa har ökat med 58 procent i jämförelse med RRV:s undersökning.
Landstingen har drabbats mest, 87 procent av samtliga landsting rapporterar incidenter, jämfört med till exempel 13 procent av statliga och kommunala bolag.

[7] Kategorin ”Manipulation” är ett samlingsbegrepp som består av manipulation av data, indata, utdata, program och registerdata.
[8] Dataintrång/datavirus innebär att respondenten i företagsundersökningen har fyllt i både dataintrång och datavirus när man beskriver brottet. Dessa har inte räknats med vilket innebär att antalet dataintrång och datavirus är fler än vad som redovisas här.

Tabell 2. Andelen drabbade inom respektive bransch åren 1997-1998 och i jämförelse med RRV:s undersökning, åren 1995-1996 (se fotnot 9).

Bransch	RRV Andel (%)	BRÅ Andel (%)
Handel	9	19
Industri	13	24
Bank/försäkringsbolag/finans	14	19
Övrig privat verksamhet	8	24
Statlig myndighet	34	51
Statligt bolag	14	13
Kommunal förvaltning	27	38
Kommunalt bolag	8	13
Landsting	57	87

I jämförelse med åren 1995-1996 (RRV) ökar andelen drabbade inom samtliga branscher utom inom statliga bolag där den minskar[9]. Den kraftigaste ökningen av andelen drabbade företag har skett inom övrig privat verksamhet.

Som framgår av tabell 3 har antalet incidenter ökat markant inom vissa branscher men minskat i andra branscher. Bland företag inom industri, handel och kommunala bolag har antalet brott och incidenter nästan fördubblats i jämförelse med RRV:s undersökning. Sammantaget har antalet brott och incidenter ökat med 75 procent inom den privata sektorn och med 15 procent inom den offentliga sektorn.

Tabell 3. Skattat antal IT-relaterade brott och incidenter uppdelade på branscher, åren 1997-1998 och i jämförelse med RRV:s undersökning, åren 1995-1996.

Bransch	RRV	BRÅ
Handel	84	166
Industri	268	526
Bank/försäkringsbolag/finans	25	27
Övrig privat verksamhet	156	216
Statlig myndighet	107	89
Statligt bolag	30	37
Kommunal förvaltning	90	123
Kommunalt bolag	16	32
Landsting	16	17
Summa	791	1 232

Den privata sektorns andel av företag som drabbats är 22 procent, i den offentliga är andelen 32 procent. Av samtliga rapporterade brott och incidenter drab-

[9] Uppgifterna för statliga och kommunala bolag är något osäkra beroende på stora successiva förändringar av populationerna.

bade 76 procent företag inom den privata sektorn och 24 procent offentlig sektor.

Den sammanlagda kostnaden för IT-relaterade brott och incidenter skattades till mellan 37,5 och 238,6 miljoner kronor[10]. Som framgår av tabell 4 ger skadorna av manipulation den enskilt största skadan per brott. Den genomsnittliga kostnaden under ett år för de företag som drabbas är cirka 140 000 kronor.

Tabell 4. Ekonomiska skador för IT-relaterad brottslighet, åren 1997-1998. Genomsnittskostnaden för de olika brottstyperna och den sammanlagda kostnaden.

	Kostnad			
	Medel (tkr)		Totalt (milj)	
Gärning	Mini	Max	Mini	Max
Dataintrång (hacking)	98,7	346,1	17,0	59,9
Manipulation	347,6	774,6	46,6	106,1
Datavirus	48,2	67,2	11,0	52,2
Stöld av information	141,3	264,8	6,9	12,9
Datavirus/dataintrång	36,1	101,9	2,5	7,1
Olovlig åtkomst	5,8	16,1	0,1	0,4
Totalt			37,5	238,6

Skadornas variation i den totala kostnaden beror dels på antalet fall, dels på skadornas omfattning. Datavirus är till antalet många men har låg kostnad per incident, medan stöld av information och manipulation har höga kostnader per incident.

De allra flesta brott och incidenter utförs av outsiders (69 procent). Räknar man bort virusangrepp och externa dataintrång (hacking), som är de vanligaste incidenterna, svarar emellertid insiders för huvuddelen av brotten och incidenterna (63 procent).

Privatpersonsundersökningen

Bland de tillfrågade privatpersonerna har 16 procent (N=1 000) drabbats av datavirus. Av dessa är det två procent som drabbats upprepade gånger. Två procent uppger att de varit utsatta för dataintrång men ingen av dem har polis-

[10] Borfallet vad avser uppgifter om kostnader är stort, för cirka 25 procent av de rapporterade incidenterna har kostnader uppgivits. *Maxvärdet* har beräknats under antagandet att de incidenter där uppgifter om kostnader saknas har samma genomsnittliga kostnad som de där kostnad angivits, vilket med största sannolikhet ger en överskattning av den totala kostnaden. *Minivärdet* har beräknats under antagandet att samtliga incidenter där inte kostnad angivits inte har medfört någon kostnad, således en definitiv underskattning.

anmält dataintrånget. Tre procent har blivit hotade eller trakasserade via e-post någon gång. Endast någon enstaka har hotats och trakasserats vid ett stort antal tillfällen.

Fem procent har sett webbsidor som innehåller uppgift om illegal drogförsäljning, fem procent har sett webbsidor som innehåller barnpornografiska bilder, 13 procent har sett nazistiska webbsidor och 9 procent har sett webbsidor som erbjuder eskortservice eller prostitution. Totalt har 28 procent sett någon av de webbsidor som BRÅ frågade efter.

26 procent av privatpersonerna upplevde brottsligheten som stor eller mycket stor på Internet. Majoriteten upplevde dock brottsligheten som ringa eller obefintlig.

Undersökningen av polisanmäld brottslighet

Den IT-relaterade brottsligheten, som leder till polisanmälan, handlar till stor del om olika sorters bedrägerier och dataintrång. Totalt i undersökningen är det 608 polisanmälningar.

Tabell 5. Polisanmäld IT-relaterad brottslighet, åren 1997-1998. Indelad efter brottstyper.

Brottstyp	Antal
Datorbedrägerier	329
Dataintrång	239
Integritetsbrott	17
Fysiska och digitala angrepp	16
Hot/trakasserier	7
Summa	608

54 procent av de anmälda brotten var bedrägerier – varav den största kategorin var kontokortsbedrägerier, 156 anmälningar. Anmälningarna om kontokortsbedrägerier på nätet har ökat kraftigt mellan åren 1997 och 1998, från 23 till 129 polisanmälningar. Majoriteten av bedrägerianmälningarna har gjorts av privatpersoner.

39 procent av samtliga polisanmälningar handlade om dataintrång, totalt 239 polisanmälningar. 60 procent av dessa var externa dataintrång och 40 procent interna dataintrång.

Enbart 7 procent av samtliga polisanmälningar gäller andra brott, vilket är en liten andel. Detta kan troligtvis förklaras med att dessa brott registreras som andra typer av brott än de som ingick i undersökningen, varför de inte finns med. Antalet IT-relaterade brott är naturligtvis betydligt fler än de IT-relaterade brott som polisanmäls.

Utifrån den polisanmälda brottsligheten är det svårt att få en bild av gärningsmännen eftersom de är så få till antalet. Sammanlagt finns 116 misstänkta

gärningsmän i brottstyperna bedrägeri och dataintrång. Endast 9 procent eller 10 personer av de misstänkta var kvinnor, vilket är en låg andel jämfört med 19 procent vad gäller samtliga brott år 1997. Uppemot hälften (41 procent) av alla misstänkta gärningsmän är mellan 15 och 20 år, jämfört med 25 procent vad gäller samtliga brott år 1997.

De vanligaste brotten

Datavirus

Datavirus är ett stort problem för företag, men även enskilda personer upplever datavirus som ett gissel. Eftersom datavirus i sig inte är olagligt är det ytterst få som leder till en polisanmälan. Av samtliga undersökta polisanmälningar finns endast en (1) anmälan angående datavirus.

I företagsundersökningen var datavirus den enskilt största rapporterade incidenten, sammanlagt 778 virusincidenter av de totalt beräknade 1 232 incidenterna. Det är 63 procent av samtliga incidenter bland företagen. Bland företagen har 47 procent av virusincidenterna kommit via Internet.

Även i de intervjuer BRÅ gjort uppges virus vara det problem som förekommer mest. Variationen är dock stor, vissa företag drabbas ytterst sällan, medan andra har dagliga virusproblem. Överlag nämns virus som ett återkommande problem bland de tillfrågade.

Knappt hälften i företagsundersökningen, som drabbats av datavirus, uppger att de inte vet vem gärningsmannen är. I de fall där företagen har kännedom om gärningsmannen är 17 procent anställda och 83 procent utomstående personer. Av de anställda är den största gruppen en person som varit anställd inom organisationen i 6-10 år (40 procent).

Såväl enskilda personer som företag drabbas av datavirus. Samtliga branscher i undersökningen har drabbats. Det skattade antalet incidenter inom den privata sektorn är 606 vilket är 77 procent av det totala antalet virusincidenter. Den offentliga sektorn har drabbats av 172 virusincidenter varav många inom den kommunala förvaltningen (38 procent eller 66 incidenter).

Av privatpersonerna har 16 procent drabbats av datavirus. Fyra uppger att de haft virus ett tjugotal gånger. Främst drabbas de som använder Internet och e-post frekvent. Av de privatpersoner, som använder e-post flera gånger om dagen, är det 27 procent som drabbats av datavirus. Av dem som surfar mycket på Internet, det vill säga mer än 30 timmar i veckan, har 54 procent drabbats av datavirus.

Förändringar

I jämförelse med RRV:s undersökning har virusangreppen ökat bland företag från 530 incidenter till 778 - en ökning med 47 procent. Inom den privata sektorn har antalet incidenter ökat med 55 procent och inom den offentliga sektorn

med 23 procent. Inom handeln och kommunala bolag har ökningen mellan de två undersökningarna varit störst, 98 respektive 150 procent.

Skador

Att drabbas av datavirus kan innebära stora kostnader för att återställa datorn eller datorsystemet till brukbart skick. För företag kan kostnaderna bestå av dels förlorade arbetstimmar på grund av att datasystemet är ur funktion, dels den arbetsinsats som krävs för att återställa systemen till ursprungsskicket. Kostnaden kan också utgöras av den förlorade information som förstörts i samband med dataviruset. För privatpersoner kan datavirus innebära att man måste lämna in sin dator för att bli av med viruset om man inte har möjlighet att själv åtgärda problemet. Av de privatpersoner som uppger att de drabbats av datavirus var tio procent tvungna att lämna in sin dator för att få den återställd.

BRÅ har skattat skadorna för företag till mellan 11 och 52,2 miljoner kronor. Det är endast ett fåtal företag som har kunnat uppskatta den ekonomiska skadan som uppkommit i samband med datavirus. Den genomsnittliga kostnaden för datavirus är mellan 48 200 och 67 200 kronor.

Säkerhet

I jämförelse med RRV:s undersökning har allt fler företag väsentligt ökat sin säkerhet. Av samtliga företag i RRV:s undersökning saknade 12 procent rutiner för att förebygga datavirus, i BRÅ:s var det endast 3 procent. När det gäller andelen inom respektive bransch har antalet företag som saknar förebyggande skydd minskat inom samtliga branscher i förhållande till RRV:s undersökning. Endast fyra procent av samtliga företag saknar rutiner och metoder för att upptäcka virus.

En markant ökning av säkerheten har alltså skett under tiden mellan de olika undersökningarna när det gäller rutiner och metoder för att förebygga och upptäcka datavirus. Att så få företag saknar skydd mot virus kan verka märkligt med tanke på frekvensen av datavirus. Förklaringen är troligtvis att de rutiner som företagen beskriver återspeglar dagsläget - de kan ha sett annorlunda ut när företagen drabbades av virusangreppet. Nuvarande rutiner kan ha tillkommit som en konsekvens av att man drabbats av IT-relaterad brottslighet och incidenter.

Hot

Av företagen upplever 67 procent datavirus som ett mycket stort eller stort hot mot deras verksamhet. Det är inte så konstigt om man ser till de resultat BRÅ:s undersökning visar. Majoriteten av de rapporterade incidenterna är just datavirus och kostnaderna för dessa är relativt stora. Vid intervjuerna med IT-chefer, säkerhetsansvariga, experter m.fl. framkommer inte samma oro för datavirus. Där är det stöld av information som upplevs som betydligt mer allvarligt för verksamheten.

Dataintrång[11]

Till kategorin dataintrång hör både externa dataintrång och dataintrång som begås internt i företaget. Interna dataintrång sker när tjänstemän överskrider sina befogenheter när det gäller åtkomst av sekretessbelagda registerupplysningar och även när anställda går in i andras datorer eller filer för att läsa, kopiera eller förstöra.

I företagsundersökningen var dataintrång den näst största kategorin av brott och incidenter efter datavirus. Sammanlagt kan antalet dataintrång bland företag med fler än 50 anställda i landet skattas till 173. Det som skulle kunnas ses som interna dataintrång i företagsundersökningen är så kallat olovligt utnyttjande av skyddsvärd ADB-lagrad information eller obehörig åtkomst. Sammanlagt finns det 25 sådana fall, utöver de andra 173 dataintrångsfallen.

I undersökningen av polisanmäld brottslighet är antalet dataintrång en relativt stor andel av samtliga polisanmälningar. Antalet dataintrång uppgår till 239, vilket är 39 procent av det totala antalet polisanmälningar avseende IT-relaterade brott. Av dessa är 81 anmälningar kategoriserade som interna dataintrång och 123 som externa dataintrång (35 anmälningar innehåller inte tillräcklig information för att kunna kategoriseras).

[11] BRÅ:s olika undersökningar skiljer sig åt på några punkter, framför allt undersökningen av polisanmäld brottslighet och företagsundersökningen. I undersökningen av polisanmäld brottslighet går det att få en klar bild av vad som skett vid intrånget, medan det i enkäten endast går att se vilka system som drabbats. Däremot ser man inte om det skett en stöld av information eller manipulation av data. Av den anledningen har det gått att mer utförligt beskriva brotten i undersökningen av polisanmäld brottslighet än i företagsundersökningen.

Tabell 6. Polisanmäld IT-relaterad brottslighet, åren 1997-1998 inom kategorin interna/externa dataintrång.

Gärning	Totalt
Dataintrång[12]	46
Manipulerat data/program	45
Raderat filer/system/program	38
Stöld av program/filer	23
Ändrat webbsida	22
Netbus/snifferprogram	21
Olovligt utnyttjande av datornät	21
Olaga registerupplysning	18
Manipulerat och raderat program/filer/data	3
Ändrat webbsida och publikation på Internet	2
Summa	239

En rad olika typer av gärningar är förknippade med dataintrång. De misstänkta gärningsmännen stjäl, manipulerar, raderar osv. De interna dataintrången skiljer sig något från de externa i den bemärkelsen att det ofta handlar om att ta fram olaga registerupplysningar vilket inte förekommer bland de externa. Enligt företagsundersökningen riktas dataintrång allt som oftast mot nätoperationssystemet (14 procent) och e-posten (29 procent). Det finns ett litet antal som drabbat webbsidor på Internet (9 procent). I de flesta fallen (77 procent) har dataintrånget skett via Internet.

Bland privatpersonerna uppger 21 att de har varit utsatta för dataintrång.

Gärningsmän och offer

Uppgifter om gärningsmän är i många fall okända eller bristfälliga. I företagsundersökningen var den misstänkte gärningsmannen en utomstående vid 83 procent av dataintrången och i 10 procent en anställd. I 90 procent av dataintrången uppges att gärningsmannen kunde betraktas som en hacker eller cracker. Obehörig åtkomst utfördes uteslutande av anställda, av dessa hade 58 procent varit anställda på företaget i mer än sex år.

I undersökningen av polisanmäld brottslighet namnges en person i 99 anmälningar av totalt 239. Av dessa 99 personer är 86 män och 11 kvinnor; i två anmälningar misstänks ett företag.

[12] Gärningen ”Dataintrång” betyder att information i polisanmälningen endast beskriver gärningen som ett dataintrång utan att någonting annat beskrivs. Det går inte att utesluta att det vid dessa dataintrång skett manipulation eller någon annan gärning. De 46 anmälningar som endast benämns dataintrång är problematiska. Troligtvis förekommer det manipulation, stöld osv. inom dessa anmälningar. Tyvärr ger inte anmälningarna tillräcklig information för att det ska gå att kategorisera in dessa under någon av de andra kategorierna.

Tabell 7. Misstänkta personers åldersfördelning i polisanmälningarna, åren 1997-1999. Uppdelat på kön.

Ålder	Kvinnor	Män	Totalt
15-19		34	34
20-24		14	14
25-29	1	5	6
30-39	1	15	16
40-49	2	9	11
>50	3	3	6
Summa	7	79	86

Som framgår av tabell 7 har endast 7 kvinnor misstänkts för dataintrång. Tre av dem är över 50 år, ingen är under 25. Bland männen är åldersgruppen 15-19 år vanligast bland de misstänkta personerna.

De misstänkta männen manipulerar, raderar och stjäl program, filer eller data (43). De gör även dataintrång (16), lägger in netbus/snifferprogram (8), utnyttjar datornät utan tillstånd (7) och ändrar webbsidor (6). De få kvinnor som finns med har tagit fram registerupplysningar (4) utan att ha behörighet till detta. I de tre övriga polisanmälningarna är alla kvinnor som har raderat filer, program eller data över 40 år. Samtliga kvinnor kan sägas ha utfört interna dataintrång.

Dataintrång drabbar, liksom datavirus, både företag och privatpersoner. Över huvud taget kan det vara svårt att få en bild av vilka som drabbas av dataintrång och om det finns någon systematik i vilka som drabbas. De externa och interna dataintrången drabbar också olika beroende på vem som är offer. Inom offentliga organisationer som polismyndigheter, landsting och kommuner är de interna dataintrången vanligare än de externa. Inom dessa organisationer är förhållandet mellan externa och interna dataintrång 45/55. Inom de övriga är det 65/35.

Av de 239 polisanmälningarna utgörs 78 procent av företag, myndigheter, kommuner, landsting och andra organisationer (se tabell 8). Antalet privatpersoner som polisanmält dataintrång är 36, det vill säga 15 procent.

Tabell 8. Polisanmäld IT-relaterad brottslighet, åren 1997-1998. Dataintrång efter anmälare.

Anmälare	Antal
Företag	96
Skola/universitet	73
Privatperson	36
Myndighet	15
Kommun/landsting	11
Förening	8
Totalt	239

Som framgår av tabell 9 är den privata sektorn mest drabbad. Av samtliga dataintrångsfall står den privata sektorn för 69 procent. Företag inom industrin är värst drabbade, därefter övrig privat verksamhet. Dessa båda står för 98 procent av dataintrången inom den privata sektorn. Företagen inom handeln har inte rapporterat ett enda fall och företag inom bank/finans/ försäkringsbolag har endast rapporterat två fall. Samtliga fall av obehörig åtkomst drabbar företag inom handeln.

Tabell 9. Dataintrång och obehörig åtkomst inom samtliga branscher, åren 1997-1998. Skattat antal incidenter (företagsundersökningen).

Bransch	Brott	
	Dataintrång	Obehörig åtkomst
Handel	0	7
Industri	75	0
Bank/finans/försäkringsbolag	2	0
Övrig privat verksamhet	42	0
Statliga myndigheter	18	7
Statliga bolag	9	0
Kommunal förvaltning	23	10
Kommunalt bolag	2	0
Landsting	1	1
Totalt privat sektor	119	7
Totalt offentlig sektor	54	18
Totalt samtliga	173	25

Kommunal förvaltning drabbas mest inom den offentliga sektorn. Den är måltavla eller har utsatts för 43 procent av samtliga dataintrång inom den offentliga sektorn. Därefter kommer statliga myndigheter (33 procent).

Förändringar

I företagsundersökningen har antalet dataintrångsfall i landet ökat i jämförelse med RRV:s undersökning. Det skattade antalet dataintrång har ökat från 117 till 173 fall, vilket är en ökning med 48 procent. Inom den privata sektorn har dataintrången ökat med 78 procent. Majoriteten av ökningen har skett inom industrin och övrig privat verksamhet.

Inom den offentliga sektorn sker det också en ökning, men en betydligt beskedligare sådan. Undantaget är kommunal förvaltning, som uppvisar betydligt fler dataintrångsincidenter åren 1997-1999 än åren 1995-1996, en ökning med 53 procent.

Av dataintrången har 69 procent av incidenterna skett via Internet, vilket är samma andel som i RRV:s undersökning.

Skador

I företagsundersökningen har skadorna för dataintrång skattats till mellan 17 och 60 miljoner kronor. Summan är högst osäker eftersom uppgifter om kostnaderna och förlusterna inte är fullständiga. Endast ett fåtal företag har specificerat sina ekonomiska skador i samband med dataintrång – och i dessa fall rör det sig om relativt stora summor. Den genomsnittliga kostnaden för dataintrång är mellan 98 700 och 346 000 kronor per fall.

I sammanlagt 12 polisanmälningar förekommer uppgifter om ekonomiska konsekvenser av dataintrången. Bland de interna dataintrången finns 7 anmälningar där det förekommer uppgifter om skador i belopp. Den sammanlagda summan för dessa uppgår till 16,5 miljoner kronor.

Det finns två fall av internt dataintrång där gärningsmännen har tillgodogjort sig stora värden dels i pengar, dels i programvara. I det första fallet har en anställd under en period av fem år förskingrat 5,7 miljoner kronor. Genom sin behörighet har den misstänkte lyckats kringgå arbetsgivarens säkerhetssystem. I det andra fallet stal en projektanställd en källkod värd 10 miljoner kronor. Dessa fall visar att möjligheten att internt stjäla eller manipulera information kan ge upphov till stora förluster för en organisation.

Det förekommer även att företag drabbas ekonomiskt av externa dataintrång. I fem polisanmälningar finns uppgifter om ekonomiska förluster. I en polisanmälan har dataintrånget lett till att man raderat cirka 9 gigabyte data från en hårddisk - en förlust för företaget på 120 000 kronor. För alla fem anmälningar är den sammanlagda summan 265 000 kronor.

Det går inte att dra några generella slutsatser utifrån materialet. Men de ekonomiska förlusterna är betydligt större vid de interna än de externa dataintrången enligt polisanmälningarna. Uttalanden från intervjupersonerna om att interna dataintrång kan ställa till större skada än externa, stämmer väl med uppgifterna i de undersökta polisanmälningarna.

Säkerhet

Jämfört med RRV:s undersökning har andelen företag som har förebyggande skydd mot dataintrång för sin verksamhet ökat från 40 till 65 procent.

Av BRÅ:s undersökning framgår att rutiner för att upptäcka dataintrång saknas i 34 procent av samtliga företag. Andelen privata företag, som saknar rutiner, är 38 procent och inom den offentliga sektorn 14 procent. Överlag är man bättre skyddad mot dataintrång inom den offentliga sektorn än inom den privata.

Av privatpersonerna har 10 procent installerat en brandvägg för att skydda sig mot dataintrång. Det kan tyckas vara få, men med tanke på vad en brandvägg kostar är det förhållandevis många trots allt.

Hot

Andelen företag som upplever dataintrång som ett mycket stort eller stort hot är 35 procent. Majoriteten (57 procent) upplever dataintrång som ett mindre hot mot verksamheten.

De flesta intervjuade företag ser det externa dataintrånget som ett hot mot företagets verksamhet, men det interna hotet anses vara betydligt större. Man har svårt att se att de externa angreppen skulle kunna leda till några större förluster. *”Den stora risken är anställda och konsulter som stjäl eller läcker information”* (person i intervjuundersökningen). Externt kan man visserligen ställa till med förtret, men att manipulera datasystemet utan att ha djupare kunskaper om systemet är mycket svårt.

Företagen har i dag en hög nivå på den tekniska IT-sidan, troligtvis har den förbättrats med åren. Däremot är den fysiska säkerheten inte särskilt hög. Följden är att det är enklare att bryta sig in för att exempelvis stjäla information än att försöka ta sig in via nätverk. Ännu bättre är att ha hjälp från en insider som kan ge vägledning om hur man kommer åt datorer och information.

Återkommande hos ett flertal av de intervjuade är att de uttrycker oro över att det faktiskt kan ha skett saker som man inte har upptäckt. Som en person uttryckte det: *”Det verkliga mörkertalet är alla de attacker som företagen inte upptäcker. Det vill säga de eventuella dataintrång som lyckats utan att man vet om att de har varit inne”* (person i intervjuundersökningen).

Manipulation[13] av data

Antalet fall av manipulation i någon form bland företagen har skattats till 137 incidenter. Det är 11 procent av samtliga brott och incidenter i företagsundersökningen. Manipulation av data, vilket betyder att man inte specificerat vilken sorts manipulation det har varit frågan om, utgör 27 procent av brotten. Därefter följer manipulation av registerdata 23 procent, manipulation av programvara 19 procent och manipulation av in- och utdata, vardera 15 procent av samtliga manipulationsbrott. Majoriteten (92 procent) av brotten har begåtts inom den egna organisationen. De system som drabbats mest är e-post (23 procent), order/lager/fakturering (12 procent) och operativ-/nätoperations-system (12 procent).

[13] Kategorin ”Manipulation” är ett samlingsbegrepp som består av manipulation av data, indata, data under bearbetning, utdata, program och registerdata. Med begreppet manipulation avses olovligt skapande, ändringar, raderingar och döljande av data med hjälp av datorn men också olovlig ändring, skapande och radering av program. I polisanmälningarna var det vanligt att interna och externa intrång ledde till att den misstänkte gärningsmannen manipulerade, raderade, stal och ändrade data och program. Dessa har därför redovisats under Dataintrång.

Gärningsmän och offer

Enligt företagsundersökningen står anställda för 65 procent av manipulationsbrotten. I 58 procent av fallen hade gärningsmannen behörighet till systemet, i 31 procent av fallen saknades behörighet.

Av 137 fall av manipulation har 116 skett inom den privata sektorn, det vill säga 85 procent. Av dessa har 87 procent drabbat företag inom handel och industri. Endast två fall har drabbat företag inom bank/finans/försäkring.

21 fall av manipulation har alltså skett inom den offentliga sektorn, det vill säga 15 procent av samtliga manipulationsbrott. Värst drabbat inom offentlig sektor är kommunal förvaltning.

Förändringar

Som tidigare visats har det skett en signifikant förändring av manipulation av data i BRÅ:s undersökning jämfört med i RRV:s. Totalt sett har manipulation bland företagen ökat, från 76 till 137 fall, vilket är en ökning med 80 procent. Det mest anmärkningsvärda är att den största ökningen sker inom den privata sektorn och att det sker en minskning inom den offentliga sektorn. I jämförelse med RRV:s undersökning har manipulationsfallen inom den privata sektorn ökat från 34 till 116 fall, det vill säga med 241 procent. Den tydligaste ökningen sker hos företag inom handeln, från 10 till 50 fall, och inom industrin, från 22 till 51 fall. Inom den offentliga sektorn har minskningen varit störst hos de statliga myndigheterna, från 17 till 5 fall. Orsakerna till dessa två förändringar är svåra att uttala sig om, men en möjlig förklaring kan vara att den offentliga sektorn uppvisar en större säkerhet när det gäller manipulation än vad den privata sektorn gör (se nedan).

Skador

De sammanlagda skadorna orsakade av manipulation av något slag inom den privata och offentliga sektorn har skattas till mellan 46,6 och 106,1 miljoner kronor. Slår man ut kostnaden per fall uppgår den ekonomiska skadan till mellan 347 600 och 774 600 kronor.

Säkerhet

Knappt hälften (47 procent) av alla företag har rutiner för att förebygga manipulation i någon form för hela verksamheten. Av samtliga företag saknar 23 procent förebyggande rutiner mot manipulation. Av de privata företagen är det 26 procent som saknar förebyggande rutiner. Av den offentliga sektorns företag är det 12 procent som saknar förebyggande rutiner.

Av samtliga företag saknar 38 procent rutiner för att upptäcka manipulation i någon form. Inom den privata sektorn är andelen företag, som saknar upptäcksrutiner, 41 procent mot 23 procent inom den offentliga sektorn. Mönstret är detsamma, den privata sektorn skyddar sig sämre än den offentliga.

Hot

Majoriteten (53 procent) av företagen upplever manipulation av något slag som ett mindre hot mot sin verksamhet. Endast 14 procent av samtliga företag ser manipulation som ett mycket stort hot mot verksamheten. I jämförelse med RRV:s undersökning kan man konstatera att hotet med manipulation av data generellt upplevs som mer påtagligt i BRÅ:s undersökning. En förklaring till detta kan vara att antalet fall av manipulation har ökat. Ser man till kostnaden för dessa brott borde företagen vara mer oroliga för manipulation än vad de uppger.

Stöld av information

Stöld av information innebär att någon stjäl eller kopierar program, data, filer m.m.[14] I företagsundersökningen skattas antalet stölder till 49, vilket är 4 procent av samtliga brott och incidenter i företagsundersökningen.

Av det totala antalet polisanmälningar finns totalt 23 anmälningar av stölder av filer och program som skett genom dataintrång. Dessa har redovisats under dataintrång (se tabell 6).

I intervjuer med IT-chefer, säkerhetsansvariga, IT-experter m.fl. har det kommit fram att stölder ofta handlar om informationsstölder av strategiskt viktiga data. De kan avse uppgifter om företagets framtida projekt, forskning, strategier och marknadsföringsplaner. Att bli bestulen på information kan få stora konsekvenser; *”Om någon får reda på utvecklingsplaner eller kommersiell information kan det vara förödande för företagets fortbestånd”* (person i intervjuundersökningen).

Informationsstöld kan också vara att en anställd tar en kopia av ett program som används inom produktionen eller stjäl företagets utvecklingsplan. En intervjuperson uppger att för några år sedan blev man erbjuden att köpa ett annat företags hela utvecklingsplan.

Hotet från insidern, när det gäller informationsstöld och de skador som kan åstadkommas, visas väl av följande fall: *”För några år sedan tog en anställd med sig information till en konkurrent som gällde ett koncept att få ner vissa kostnader. Genom konceptet hade man själva lyckats sänka kostnaderna med mycket stora belopp. För det konkurrerande företaget bör informationen vara värd betydligt mer”*(person i intervjuundersökningen). Fallet visar värdet på den information som finns hos ett företag. Problemet för gärningsmannen är att få informationen omsatt i pengar. På ett företag berättade man att en anställd kopierade teknisk utvecklingsinformation och försökte sälja den till ett konkurrerande företag.

Andra stölder är att företagen har blivit av med datorer: *”Vi har blivit av med datorer från vårt huvudkontor. Då ställer man sig alltid frågan om det*

[14] Begreppet används inte i straffrättslig utan i kriminologisk mening. Stöld kan inte ske av något immateriellt. Stöld av information rubriceras i stället som företagsspionage etc.

var vanliga datortjuvar eller om det var några andra. Den frågan får man inte svar på eftersom ingen har åkt fast"(person i intervjuundersökningen). Ett sätt att få sådana misstankar bekräftade är att man upptäcker information där den inte borde finnas.

Gärningsmän och offer

Uppgifter om gärningsmännen förekommer endast i företagsundersökningen. I 30 procent av samtliga stölder eller kopiering saknas uppgifter om gärningsmän. I de fall där det finns en gärningsman har brotten till största delen utförts av insiders (70 procent). Nästan samtliga av dessa (85 procent) har haft behörighet till det aktuella systemet. Företag inom industrin drabbas mest av informationsstöld. Av samtliga stölder står de för 78 procent av fallen. Därefter kommer statliga bolag och bank/finans/försäkringsbolag med 6 procent och kommunala bolag med 4 procent.

Förändringar

Antalet informationsstölder bland företagen har ökat med 22 procent i jämförelse med RRV:s undersökning från 1995-1996. Antalet informationsstölder ökar bland företag inom den privata sektorn och framför allt inom industrin. Inom den offentliga sektorn minskar antalet stölder av information med 27 procent.

Skador

Som tidigare nämnts kan informationsstöld leda till stora ekonomiska förluster och skador. Stjäls viktig strategisk information från ett företag kan det äventyra verksamhetens fortsatta existens. Att uppskatta värdet på information kan vara problematiskt. Kortsiktigt kan information värderas, men långsiktigt är det svårt att värdera konsekvenserna av att viss information stjäls.

Varje incident kostar i genomsnitt mellan 141 300 och 264 800 kronor. Beroende på att antalet fall är litet blir dock de totala kostnaderna inte så stora, skadorna har skattats till mellan 6,9 och 12,9 miljoner kronor.

Säkerhet

I företagsundersökningen ställs inga frågor om företagen har rutiner för att upptäcka eller förebygga informationsstölder. Den fråga som berör säkerheten angående stölder gäller om företagen har rutiner för att rapportera att sådana brott ägt rum. I 47 procent av samtliga företag saknas rutiner för att rapportera informationsstöld. Inom samtliga branscher, med undantag av bank/finans/försäkring, är det knappt hälften eller mer än hälften av företagen som saknar rapporteringsrutiner. Inom bank/finans/försäkring är det 21 procent av företagen som saknar dessa rutiner. Resultatet är anmärkningsvärt med tanke på konsekvenserna av om strategisk information stjäls eller kopieras.

Hot

Av samtliga företag uppger 37 procent att informationsstöld är ett mycket stort eller stort hot mot verksamheten. Över hälften (53 procent) anser att det är ett mindre hot mot företagets verksamhet. Uppdelat på privat och offentlig sektor ser andelarna i stort sett lika ut. Bransch för bransch kan man konstatera att 51 procent av företagen inom bank/finans/försäkringsbolag upplever informationsstöld som ett mycket stort hot eller stort hot mot verksamheten. Även landstingen uppvisar en större hotkänsla. Att den finansiella sektorn upplever informationsstöld som ett hot är inte så konstigt, däremot är det anmärkningsvärt att övriga företag inte ser detta som ett stort hot. Enligt vad företrädare för företagen säger i intervjuerna är just informationsstöld ett hot som upplevs kunna leda till de största skadorna för företaget.

Bedrägerier

Två av BRÅ:s undersökningar berör bedrägerier – undersökningen av den polisanmälda brottsligheten och privatpersonsundersökningen.

På Internet förekommer falska webbsidor där ”företaget” utger sig för att sälja varor av olika slag, till exempel mobiltelefoner och datorkomponenter.

Kontokortsbedrägeri innebär att någon okänd använt anmälarens kontokortsnummer för att köpa varor på Internet.

I undersökningen av polisanmäld brottslighet finns en relativt stor grupp gärningsmän som ägnar sig åt att stjäla andras Internetkonton och koder för att kunna surfa utan kostnad, så kallade frisurfare. En frisurfares motiv kan vara av två slag. Det ena är att undandra sig kostnaden för den tid som frisurfaren är uppkopplad, det andra är att vilja dölja sin identitet bakom någon annans. Frisurfaren, som vill undvika debitering, är troligtvis en storkonsument av Internet. Det andra motivet kan exemplifieras av den så kallade örebropedofilen som utnyttjade en persons Internetkonto för att sprida barnpornografiska bilder och därmed försöka undgå upptäckt.

Gemensamt för samtliga polisanmälningar inom denna kategori är att brotten skett på Internet eller via e-post.

Tabell 10. Polisanmäld IT-relaterad brottslighet, åren 1997-1998 inom kategorin "Bedrägeri på Internet". Uppdelat på gärningstypologi.

Gärning	Antal
Kontokortsbedrägeri	156
Frisurfande	107
Falsk varuförsäljning via webbsida	38
Använt annans e-postkonto	10
Handlat varor i annans namn (exkl. kontkort)	8
Falsk fakturering	8
Social engineering[15]	1
Obehöriga kontobelastningar via Internet	1
Summa	329

Antalet polisanmälda bedrägerier på Internet uppgår till 329, vilket är 54 procent av det totala antalet polisanmälningar. Som framgår av tabell 6 är det två sorters brott som dominerar; kontokortsbedrägerier (47 procent) och frisurfande (32 procent). Dessa brott står för 80 procent av det totala antalet polisanmälningar inom kategorin. Därefter kommer falsk varuförsäljning via webbsida (12 procent).

Av privatpersonerna uppger två att de har blivit lurade när de har handlat på nätet. Sex personer har råkat ut för obehöriga debiteringar när de utnyttjat avgiftsbelagda tjänster på Internet. Endast 7 procent som hade handlat kunde också uppge betalningssätt. Majoriteten av dessa (68 procent) har använt postförskott eller faktura. Omkring 14 personer har använt sitt kontokortsnummer och av dessa har tio lämnat ut hela numret via Internet, resterande via fax eller på annat sätt.

Gärningsmän och offer

Av de 329 polisanmälningarna innehåller 45 uppgifter om misstänkt gärningsman[16]. Av dessa är 32 män, tre kvinnor och nio företag. Misstänkta företag har i fem fall anmälts för falsk webbsida, i tre fall för falsk fakturering och i ett fall för kontokortsbedrägeri.

De misstänkta männen har i 17 fall anmälts för falsk webbsida och falsk varuförsäljning. Vidare är det tio fall av frisurfare. De tre misstänkta kvinnorna

[15] Termen social engineering beskriver de knep som gärningsmän använder för att komma över viktig information för att kunna utföra ett dataintrång. Det kan också vara ett sätt att få personer att lämna ut hemlig information. Tekniker som används är till exempel att utge sig för att vara en chef på ett stort företag som behöver en viss information från en underordnad (Parker, 1998).

[16] En förklaring till det låga antalet misstänkta gärningsmän kan antas vara att det är först efter en polisanmälan som banken eller kontokortsföretaget påbörjar en utredning.

har i ett fall anmälts för kontokortsbedrägeri, i två fall har de använt annans e-postkonto.

Av de 45 anmälningarna med en misstänkt gärningsman, innehåller 30 information om den misstänktes ålder. Som framgår av tabell 11 är den enskilt största delen av gärningsmännen inom åldersgruppen 15-19 år.

Tabell 11. Misstänkta personers åldersfördelning i polisanmälningarna, åren 1997-1999. Uppdelat på kön.

Ålder	Kvinnor	Män	Totalt
15-19	2	12	14
20-24	-	7	7
25-29	-	3	3
30-39	-	2	2
40-50	1	3	4
Summa	3	27	30

Av 329 polisanmälningar har 282 gjorts av privatpersoner, vilket motsvarar 85 procent av samtliga anmälningar. Privatpersoner anmäler flest kontokortsbedrägerier. Antalet polisanmälningar om kontokortsbedrägerier uppgår till 152, vilket är 54 procent av anmälningarna. Därefter kommer fall där någon använt anmälarens Internetkonto och surfat gratis (75), frisurfande. Det finns 33 anmälningar om falska webbsidor där man säljer fiktiva varor. Övriga anmälningar uppgår till 22, varav nio avser användningar av annans e-post och sju falsk fakturering.

Företagen står för 11 procent (35) av anmälningarna avseende bedrägerier på Internet. Det vanligaste brottet som anmälts är att gärningsmannen surfar gratis genom att utnyttja företagets Internetkonto (21), därefter följer falsk varuförsäljning (5), kontokortsbedrägerier (4), gärningsmannen har beställt varor i företagets namn (4) och falsk fakturering (1).

Förändringar

Det finns en kraftig förändring av de polisanmälda bedrägerierna mellan åren 1997 och 1998. Antalet anmälningar ökar från 94 år 1997 till 235 år 1998. Det är en ökning med 150 procent.

Privatpersoner anmälde år 1997 sammanlagt 72 brott och år 1998 210 brott, en ökning med 192 procent. Antalet anmälda kontokortsbedrägerier har ökat med drygt 400 procent, från 23 till 129. Det framgår också av polisanmälningarna att antalet falska webbsidor med fiktiva varor ökar och antalet frisurfande minskar mellan åren 1997 och 1998.

Eftersom tidsperioden är endast två år, är det svårt att uttala sig om det har skett någon faktisk ökning av brottsligheten. Vad som kan sägas är att andelen kontokortsbedrägerier har ökat markant. Det är högst sannolikt att det skett en faktisk ökning av kontokortsbedrägerierna på Internet. Det är rimligt att ökningen kan förklaras med utvecklingen av näthandeln och därmed användning-

en av kreditkort som betalningsmedel och att den ökning som finns i materialet speglar denna utveckling. Ytterligare en förklaring kan vara att tekniker att begå dessa brott har spritt sig och därmed medfört att kontokortsbedrägerierna ökat.

Skador

I 212 polisanmälningar av 329 förekommer uppgifter om ekonomiska förluster för målsäganden. Den sammanlagda summan för dessa 212 anmälningar uppgår till 1,5 miljoner, en genomsnittssumma på cirka 6 937 kronor per polisanmälning. De polisanmälda bedrägerier som förorsakat störst ekonomiska förluster är frisurfande (668 168 kr), därefter följer kontokortsbedrägerier (592 455 kr).

Säkerhet

Privatpersonerna tillfrågades om de upplever att det är säkert att handla på Internet. Av de tillfrågade upplever 42 procent Internethandeln som osäker, 12 procent upplever den som delvis osäker och 23 procent upplever att det är säkert att handla på Internet. Majoriteten (74 procent) anser att det är osäkert att lämna ut kontokortsnumret på Internet. Majoriteten (69 procent) av de tillfrågade använder inte Internet för att köpa varor. Sammanfattningsvis kan man säga att förtroendet för säkerheten påverkar viljan att använda Internet som en marknadsplats. Men av dem som handlar på Internet uppger 95 procent att de kommer att handla mer på Internet.

Övriga brott

Med övriga brott avses brott som inte är så vanliga men som ändå kommit fram i BRÅ:s olika undersökningar.

Fysiska och digitala angrepp

Fysiska och digitala angrepp avser allt från fysiska sabotage mot datorutrustning till sabotage via Internet eller e-post. De brott som enligt svensk straffrätt troligtvis aktualiseras är ofredande och i vissa fall sabotage.

Antalet polisanmälningar med fysiska och digitala angrepp uppgår till 15 varav åtta avser mailbombning, fem fysiskt sabotage av hårddisk och 2 denial of service[17]. Skolor och universitet står för hälften av anmälningarna, företag

[17] Begreppet innebär att någon ser till att en annan användares dator får icke önskvärd information i en sådan mängd att datorn inte klarar att bearbeta mängden information. Resultatet blir att systemet inte går att använda. (Telia, 1998)

för tre, privatpersoner för två, föreningar för en, kommuner och landsting för en och myndigheter för en polisanmälan.

Hot och trakasserier

Genom e-post och Internet har det kommit nya möjligheter att hota eller trakassera enskilda personer eller organisationer. En av polisanmälningarna i undersökningen ger ett exempel på hur hot kan ta sig nya former och uttrycksmöjligheter. En nazistisk webbsida pekade ut en viss person och sa att han skulle akta sig. I detta fall gällde anmälan dels hot mot personen i fråga, dels behandling av personuppgifter utan samtycke.

Sammanlagt finns det sju polisanmälningar avseende hot i materialet. Tre avser olaga hot, varav två mot tjänsteman. En polisanmälan avser olaga hot mot barn under 18 år och en dataintrång. Privatpersoner står för fem av polisanmälningarna, de övriga två kommer från polismyndigheter.

Det begränsade antalet polisanmälningar kan troligtvis förklaras av att polisanmälningar med aktuella brottskoder inte samlades in av BRÅ. Det är högst troligt att antalet olaga hot via e-post och Internet är betydligt fler än vad som kommit fram här[18].

Av privatpersonerna framkom att tre på hundra har blivit hotad eller trakasserad via e-post. Några av dessa uppger att de blivit utsatta för upprepade hot eller trakasserier. En uppger sig ha blivit utsatt för ett 30-tal trakasserier via e-post.

Integritetsbrott

Kategorin integritetsbrott hänvisar till 20 § datalagen (1973:289) och till kategorin integritetsskyddsbrott i polisens registrering. Under kategorin integritetsbrott är det endast upprättande av personregister[19] eller publicering av personuppgifter på Internet som redovisas.

Antalet integritetsbrott i materialet är 17, vilket är tre procent av den totala volymen av anmälningarna. Av dessa är åtta olaglig registrering av personuppgift, det vill säga ett personregister utan tillstånd. Det finns nio polis-

---

[18] För att få en uppfattning om hur vanligt olaga hot via e-post eller Internet är bör man ha i åtanke att antalet anmälningar av olaga hot för året 1997 uppgick till 30 248. Möjligheten att undersöka samtliga dessa fall, för att konstatera kopplingen till IT, har inte funnits inom det här projektets ramar.

[19] För att upprätta ett personregister krävdes licens/tillstånd från Datainspektionen. Fanns inte detta bröt personen eller företaget mot lagen. I oktober 1998 trädde personuppgiftslagen (PUL) i kraft vilket bland annat medförde att det blev förbjudet att publicera personuppgifter på Internet utan personens medgivande.

anmälningar om att någon lagt ut personuppgifter på Internet utan medgivande. I tio av de 17 anmälningarna är det en privatperson som polisanmält.

Övrigt

Privatpersonerna (1 000 personer) tillfrågades om de via e-post blivit erbjudna att köpa illegala varor av något slag. När det gäller piratkopierade program och spel uppger 57 personer att de har fått sådana erbjudanden. Billiga cigaretter uppger 27 personer att de har fått erbjudanden om, billig sprit 17 och erbjudanden om att köpa narkotika har sju personer fått. En person har fått erbjudanden om att köpa barnpornografiska bilder. Två personer har blivit erbjudna att köpa vapen. Sammantaget är det tio procent av intervjupersonerna som har blivit erbjudna något av detta över huvud taget.

Privatpersonerna tillfrågades också om de träffat på något av följande: webbsida/bilder med barnpornografi, nazistisk webbsida, prostitution/ eskortservice och illegal drogförsäljning.

Fem av hundra har sett barnpornografi på Internet. Tolv av hundra uppger att de stött på en nazistisk webbsida. Nio av hundra har kommit i kontakt med webbsidor om prostitution eller eskortservice och fem av hundra har sett illegal drogförsäljning. Totalt har 28 procent av samtliga träffat på någon av de listade företeelserna.

Brottsligheten och polisen

Privatpersonerna tillfrågades om hur de upplevde brottsligheten på Internet. Totalt uppger 26 procent att brottsligheten är stor eller mycket stor, medan 49 procent uppger att brottsligheten är alltifrån liten till obefintlig. 25 procent har ingen uppfattning eller är tveksamma. Däremot är det många som uppger att polisens resurser är för små; endast nio procent uppger att polisens resurser är tillräckliga. Troligt är att svaren ska tolkas så att man har svarat på den första frågan utifrån egna erfarenheter och på den andra frågan utifrån en allmän uppfattning om resursbrister inom polisen.

I intervjuer med IT-chefer, säkerhetsexperter m.fl. framträder ett allmänt missnöje med de rättsvårdande myndigheterna. En av frågorna handlar om hur man ser på polisens resurser och hur relationen till polisen är. Svaren är tvådelade; å ena sidan har man ett gott samarbete med polisen, å andra sidan uppger man att polisens resurser inte räcker till. En intervjuperson säger i ett talande exempel att: *”Vi anmäler i princip allt till polisen och Finansinspektionen. Vi anmäler trots att vi vet att ingenting händer. Polisen kommer inte utreda”*. En annan menar att *”Vad kan polisen göra? Man räknar inte med någon hjälp från polisen på detta område. Det vore bra om polisen skaffade kompetens på IT-området”*.

Däremot anser man att man har bra kontakt med polisen. En intervjuperson beskriver förhållandet till polisen:*” Vi har ett stort förtroende för polisen. Men jag kan säga så här; om vi bara kan se att vi får mer besvär och inte ser någon nytta, varför ska vi då gå till polisen?”* Besvären intervjupersonen talar om är att utredningar tar lång tid och att det inte finns kompetens och resurser för dessa brott. Just dessa faktorer pekar i stort sett samtliga intervjupersoner på. Nyttan av att anmäla återkommer: *”Brottsutredningar tar lång tid, det finns taskig kompetens och stora brister. Det måste finnas ett visst mått av egennytta för att man ska samarbeta med polisen”*.

Anmälningsbenägenhet

Men att viljan att anmäla IT-relaterad brottslighet är låg beror också på en rad andra olika faktorer. En sådan faktor tycks vara att det är känsligt för företag att gå ut med att man drabbats av dataintrång i sina datasystem. *”Pinsamma brott anmäls inte till polisen. Skälet är att undvika dålig publicitet”*.

En av intervjupersonerna pekar på två förklaringar till varför man inte anmäler: *”… man vill inte figurera och vad kan polisen göra?”*. En annan menar att: *”Anmälan skapar ”badwill” för företaget, men också kostnader i tid för företaget att ställa upp på polisens utredning. Detta leder till att de företag som har kapacitet och ekonomisk möjlighet utreder själva”*.

Problemet kan lösas inom det egna företaget. Man utreder själv. *”Vi gör så här; eftersom vi är ett så pass stort företag så utreder vi det mesta själva och lämnar allt till polisen med namn, adress, telefonnummer, tidsaspekter m.m.”*. Det framgår av intervjuerna att samarbete förekommer mellan stora företag. Flera nämner att man har ett gemensamt intresse av att samarbeta med varandra. *”Incidenter anmäls sällan till polisen utan man håller det internt. Däremot utbyter storföretagen emellan information om incidenterna.”*

Men det verkar även vara så att problemet med kompetens inte bara gäller polisen. En person beskrev problemet på detta sätt: *”I dag har polisen inga resurser. Få personer inom de rättsvårdande myndigheterna har den kunskap som behövs för att förstå brottsligheten och hur brotten genomförts. Bristen på kunskap följer med hela vägen i rättsprocessen, från polisanmälan in i domstolsförhandlingen.”*

I företagsundersökningen anmäls endast 12 procent av samtliga IT-relaterade brott och incidenter. Det låga talet kan förklaras av det stora antalet datavirus. Exkluderas virus stiger antalet fall som polisanmäls till 33 procent.

Det finns ett antal faktorer som påverkar anmälningsbenägenheten när det gäller brott generellt. De två viktigaste anses vara skadans grovhet och den sociala relation som finns mellan offer och gärningsman. När offer och gärningsman är nära bekanta är benägenheten att anmäla mindre än om så inte är fallet. När det gäller egendomsbrott skiftar benägenheten att anmäla beroende på skadans grovhet och om det finns försäkringsskydd, men även beroende på vem som är offer. Brott som innebär stora skador leder oftare till polisanmälan än brott med mindre skador. Andra faktorer som kan påverka viljan att anmäla

brott kan vara den allmänna synen på brottsligheten och i vilken mån brottstypen uppmärksammas av medierna (BRÅ, 1998:22-23). När det gäller den IT-relaterade brottsligheten påverkas viljan att anmäla också av att företaget kan uppfatta det som känsligt att man blivit drabbad av sådan brottslighet, en uppfattning som tydligt framgår av intervjuerna, men det kan också finnas en tvekan om man verkligen blivit utsatta för brott. När det gäller IT-relaterad brottslighet kan svårigheter uppkomma när det gäller att fastställa var brottet begåtts. Detta leder till oklarheter som kan inverka på viljan att anmäla till polisen. Att anmäla påverkas också av anmälarens förtroende för polisens kompetens på området och därmed indirekt möjligheterna att utreda brotten.

IT-relaterad brottslighet: Diskussion

Gamla brott i nya kläder?

Är IT-relaterad brottslighet en ny form av brottslighet? Eller är det samma gamla brott men i ny teknisk och samhällelig miljö?

BRÅ:s uppfattning, efter att ha genomfört undersökningarna av faktiska brott, är att den IT-relaterade brottsligheten till stor del handlar om traditionella brott i ny teknisk miljö.

Men det kan finnas skäl att särskilja vissa brott som mer genuina ”databrott” än andra. Det gäller intrång i datorer eller nätverk och sådana brott som sker via dataintrång. Brottet sker helt och hållet i datormiljön, vilken också är en förutsättning för brotten. Den digitaliserade informationen, som inte fanns före datorerna, kan stjälas, förstöras eller manipuleras. Det finns också särskilda moderna brottstyper för dessa förfaranden. Det gäller databedrägeri och dataintrång.

Men även dessa brott kan sägas ha sina traditionella förebilder. Man kan utan lov ta sig in i exempelvis ett kontor, öppna arkivskåpet och kopiera, ändra eller förstöra dokument. Även moderna brott, som förutsätter datormiljö, är således i grunden traditionella brott.

Men dessa slutsatser innebär inte att allt kan stanna vid det gamla. Det moderna risksamhället ställer krav på ökad vaksamhet och insatser mot en brottslighet som utnyttjar den moderna tekniken. Dessa frågor utvecklas nedan.

Som nämnts är IT-relaterad brottslighet en samlingsbeteckning på brott där IT är med i bilden. Beteckningen kan på sin höjd anses vara relevant i dag då det finns behov av att skilja den moderna brottsligheten från den traditionella. Med tiden kommer beteckningen IT-relaterad brottslighet att sakna betydelse eftersom fler och fler brott på ett eller annat sätt kommer att ha beröring med IT, som en följd av att den moderna tekniken i allt högre grad genomsyrar samhällets alla delar.

Vad betyder den IT-relaterade brottsligheten för oss? Är den allvarlig?

Virus är ett gissel

De incidenter som drabbar flest privatpersoner och företag är utan tvekan virus. Incidenterna har ökat som en följd av att allt fler är uppkopplade till publika nät. Virus orsakar mycket besvär och grus i maskineriet hos de drabbade. Kostnaderna är stora för att återställa datasystemen i brukbart skick.

Det moderna samhällets värden ligger i information

Om virus är IT-samhällets gissel som drabbar stora användargrupper, utgör dataintrång det stora hotet mot enskilda användare. För företag är dataintrång kvantitetsmässigt den näst största kategorin brott och incidenter efter virus. Dataintrång hotar det moderna samhällets kanske största värde, information. Det är också ett brott som kännetecknas av den nya teknikens karaktäristika; oberoende av tid och rum, möjlighet att komma över närmast obegränsade mängder information, verklighetsfrämmande brott långt från brottsoffren etc.

IT-chefer och andra befattningshavare bekräftar informationens stora betydelse för företagen och att man ser allvarligt på stöld, manipulation och radering av information.

Bedrägerierna har hittat ut på nätet

Eftersom handel sker på nätet och köparen ska uppge kontokortsnummer, förekommer det att personer utnyttjar andras kontokortsnummer. Det är ofta oklart hur gärningsmannen kommit över kontokortsnumren. Eftersom Internet fungerar som ett globalt marknadstorg är det en följdriktig utveckling att falska varor och tjänster bjuds ut på nätet.

Hot och trakasserier kan skickas via e-post

E-post och Internet har skapat nya förutsättningar för kommunikation men också nya sätt att hota eller trakassera enskilda personer eller företag. Tre på hundra privatpersoner med Internetabonnemang har utsatts för hot eller trakasserier via e-post.

Nätet fungerar som ett globalt marknadstorg för illegala varor eller budskap

Internet och e-post har skapat nya förutsättningar för marknadsföring, köp och försäljning av varor och tjänster. Det gäller även på den illegala marknaden. Idéer och budskap kan föras ut över hela världen, vilket också utnyttjas för att sprida propaganda. Det är billigt, särskilt i förhållande till hur många som nås, och det är svårt för världssamfundet att förhindra och förbjuda spridning.

Samtidigt som förutsättningarna är stora för att torgföra varor, tjänster och budskap innebär de publika näten en risk för att upptäckas av de brottsbekämpande myndigheterna, vilket kan ha en återhållande effekt. BRÅ:s undersökningar visar trots allt att det stora flertalet av privatpersonerna med Internetabonnemang inte har kommit i kontakt med webbsidor som innehåller barnpornografi, nazistisk propaganda, prostitution och eskortservice samt drogförsäljning.

Den IT-relaterade brottsligheten utgörs till största delen av vardagsbrott

Som med annan brottslighet utgörs den IT-relaterade brottsligheten till största delen av vardagsbrott, det vill säga tämligen vanliga brott. Även om dessa brott många gånger är allvarliga är de i straffrättsligt hänseende sällan grova.

Men det hindrar inte att mycket allvarliga brott sker

På samma sätt som med traditionell brottslighet är de grova brotten sällsynta. Några sådana brott har kommit fram i BRÅ:s undersökningar, det gäller bland annat stöld och manipulation av information.

Framtiden

Samhället blir mer och mer beroende av information. IT kommer i allt högre grad att genomsyra våra liv. Fler och fler brott kommer att kunna karaktäriseras som IT-relaterade. Teknikkunnandet ökar, IT blir mer standardiserad och användarvänlig, tekniken tar allt mindre plats och blir mer och mer mobil. Nätverken knyter ihop ”the global village”.

Mot bakgrund av att brotten kan utföras från vilken plats som helst och potentiellt av ett stort antal datakunniga personer, kan nå praktiskt taget alla och ställa till med stor skada, kan den IT-relaterade brottsligheten i framtiden komma att bestå av allvarligare brott och hot än vad som nu är fallet (Sieber, 1998). Det kan handla om att använda tekniken i politiskt syfte, eller att komma över värdefull information som ett led i bland annat industrispionage eller finansiell information för att få ut pengar (NCIS, 1998). Men det finns bedömare som menar att Internet är relativt säkert och att det inte finns anledning att slå larm (Adamski, 1999). Det är också viktigt att betona att även säkerhetssystem av olika slag drar nytta av teknikutvecklingen och att både det brottsförebyggande och bekämpande arbetet förbättras genom IT.

I informationssamhället ökar betydelsen av mjukvaror som program, musik och film. Piratkopieringen kommer att fortsätta att vara ett ekonomiskt hot mot upphovsrättshavare.

Internet har flera egenskaper som gör det intressant för bedrägeri-, budskaps- och svindleribrott. Det är billigt, har stor spridning, man kan vara anonym och det är svårt att värdera vilka resurser och vilken sanningshalt som ligger bakom investeringserbjudande etc. Dessa faktorer, i takt med en ökad användning av Internet, bör kunna leda till flera sådana brott. Internet och andra nät kommer mer och mer att användas som en mötesplats. Det handlar om utbyte av information i brottsliga syften, om att bjuda ut förbjudna varor, komma i kontakt med kunder och likasinnade, sprida olagliga budskap m.m. Näten blir ett medium som skapar förutsättningar för möten över gränserna. Brotten sker nu globalt. Samtidigt skapar näten nya förutsättningar för spaning. Kanske kommer de rättsbekämpande myndigheterna runt om i världen att hålla

tillbaka kriminaliteten på nätet. Men det är starka krafter att kämpa mot. Ett framtidshot som ibland lyfts fram är den globala organiserade brottsligheten, som kan kontrollera en betydelsefull del av våra liv, och terrorismen (Castells, 1998).

Slutsatser och förslag

Slutsatser

BRÅ:s undersökningar ger inte belägg för att den IT-relaterade brottsligheten skulle vara så omfattande och allvarlig som den mytologiserade bild man gärna skapar av den. I stället framträder bilden av en IT-relaterad brottslighet av närmast ”vardagskaraktär”. Detta hindrar inte att det förekommit ett antal grova brott, bland annat där stora värden stått på spel.

Även om det således finns skäl att vara skeptisk till de farhågor som redovisats om den IT-relaterade brottsligheten och den framtida hotbilden av denna brottslighet, finns också grund för att ta den på allvar. Det gäller främst förekomsten av strukturella förändringar som skapar nya tillfällesstrukturer för allvarliga brott. Det framgår tydligt hur viktig information är i samhället och näringslivet har i några fall utsatts för stölder av strategisk information. Det finns därför skäl att öka insatserna mot den IT-relaterade brottsligheten.

Förslag

Egenåtgärder

Förebyggande arbete är det effektivaste sättet att skydda sig mot brott, vare sig det är IT-relaterad brottslighet eller inte. Men i informationssamhället kommer förebyggande åtgärder att vara ännu viktigare än i dag. Globaliseringen, nationsgränsernas minskade betydelse och nätverkens gränsöverskridande karaktär medför att traditionella straffrättsliga lösningar kommer att ha liten betydelse för att minska den IT-relaterade brottsligheten. Tekniska säkerhetsstandarder, olika behörighetsnivåer, säkerhetspolicy- och instruktioner, ökad medvetenhet hos användarna och utbildning är viktiga inslag i det brottsförebyggande arbetet.

Informationens värde – ökad medvetenhet

Det är förvånande att så många som över hälften av företagen i företagsundersökningen anser att informationsstöld utgör ett mindre hot mot den egna verksamheten. Enligt BRÅ:s uppfattning är detta ett tecken på underskattning av värdet på den information som företagen hanterar. Eftersom information kanske är den moderna tidens största tillgång, bör särskild uppmärksamhet riktas mot att förebygga stöld av information. Medvetenheten om riskerna bör höjas

generellt i samhället. Det gäller inte enbart att förebygga stöld av information utan också att förebygga manipulation och dataintrång. Men även på andra nivåer bör informationens ökade värde få genomslag. Det gäller hos statsmakterna, i lagstiftningen och hos de brottsbekämpande myndigheterna.

Utbildning och kompetens

Det brukar heta att det krävs utbildning, särskilda enheter osv. när nya företeelser uppkommer. Så har det också sagts om IT och brottsbekämpning. Men IT genomsyrar i dag hela samhället. IT är därför inte längre ett område enbart för specialister. Det innebär att IT måste var ett naturligt inslag i all brottsförebyggande och brottsbekämpande verksamhet. Detta motsäger inte att det också kan krävas spetskompetens inom rättsväsendet.

Tekniska och organisatoriska lösningar

IT-relaterade brott är till stor del en fråga om tekniska och organisatoriska problem. De förebyggande lösningarna måste därför också i hög grad vara av teknisk och organisatorisk natur.

Den mänskliga faktorn

Men att skydda sig mot IT-relaterad brottslighet kan inte enbart reduceras till en fråga om tekniska och organisatoriska lösningar som brandväggar, lösenord och ökad kontroll samt utbildning i säkerhetstänkande. Eftersom insiderhotet är störst måste också människan komma i centrum. Att arbeta med att främja en öppen dialog på arbetsplatsen och skapa organisatoriska lösningar, som minskar spänningarna mellan olika nivåer, är viktiga inslag i ett säkerhetstänkande.

Internationellt samarbete

Eftersom IT inte känner några nationsgränser är det internationella samarbetet av grundläggande betydelse för att motverka och bekämpa IT-relaterad brottslighet. Förebilder finns på andra gränsöverskridande områden som exempelvis sjö- och luftfart, tullsamarbete och miljöfrågor.

Någon måste ta ett huvudansvar

På det nationella planet bör ett större ansvar tas för att förebygga brott, genom att sprida information om hur man skyddar sig etc. I dag är det flera myndigheter som hanterar säkerhetsfrågor. Det är naturligt med många aktörer eftersom IT utgör en integrerad del av samhället. Men det vore en fördel om ansvaret för IT-säkerheten blev tydlig, till exempel att någon myndighet fick ett huvudansvar för datasäkerheten. En myndighet som sedan kunde samverka med andra myndigheter, kommuner, organisationer och – inte minst – med näringslivet.

Ökad närvaro i den virtuella världen

Liksom polisen patrullerar och spanar i den verkliga världen bör även den virtuella världen kontrolleras eftersom allt fler brott kommer att ske på nätet. För att komma åt den mer avancerade brottsligheten krävs en satsning på underrättelsetjänst.

Litteratur

Adamski, Andrzej (1999). *"Crimes Related to the Computer Network. Threats and Opportunities: a Criminological Perspective"*. In Five Issues in European Criminal Justice. Ed. Joutsen, Matti. Heuni.

Alberganti, Michel (1999). *Les sites gouvernementaux américaines victimes d´attaques musclées.* Le Monde den 2 juli 1999.

Adamoli, Sabrina. m.fl.(1998). *Organised crime around the world*. Transcrime. Heuni.

Alalehto, Tage. (1999). *Motiv eller tillfälle?* En studie om ekonomisk brottslighet i restaurangbranschen. Stockholm.

Arbetsgruppen om Informationskrigföring (AgIW) (1997). *Åtgärder och skydd mot informationskrigföring*. Rapport 1 från arbetsgruppen om informationskrigföring. Stencil 1997-08-15.

Arbetsgruppen om Informationskrigföring (AgIW) (1998). *Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning m.m*. Rapport 2 (hemlig) från arbetsgruppen om informationskrigföring. Stencil 1998-05-29.

Audit Commission (1999). *Ghost in the machine. An analysis of IT fraud and abuse*. Audit Commission update. February 1999.

Brottsförebyggande rådet (1998). *Konsten att läsa statistik om brott och brottslingar*. BRÅ, Stockholm

Castells, Manuel (1996). *Nätverkssamhällets framväxt. Informationsåldern. Ekonomi, samhälle och kultur.* Band 1. Daidalos.

Castells, Manuel (1998). *End of the Millennium. The Information Age: Economy, Society and Culture,* del 3. Blackwell.

Clarke, Roger (1998) *Technological aspects of Internet crime prevention*. Paper till Australian Institute for criminolog´s conference on "Internet Crime", Melbourne university, 16-17 February 1998.

Cornils, Karin (1999). *Om lokalisering av brott på Internet*. Nordisk Tidsskrift for Kriminalvidenskab.

CSI (1999). *Computer security. Issues & Trends*. Computer Security Institute (CSI). Vol V, no 1.

Davidsson, James. D. och Rees-Mogg, William. (1997). *The sovereign individual.* Pan Books.

Falletti, Francois och Debove, Frédéric. (1998). *Planète criminelle. Le crime, phénomène social du siècle?* Criminalité internationale. Presses universitaires de France.

Grabosky, Peter; Smith, Russel. G. och Wright, Paul (1998). *Nouvelles technologies, nouveaux délits.* Risque et information. Les cahiers de la securité intérieure, no 34, IHESI.

Hallinger, Richard C. (1997). *Crime, deviance and the computer*. Dartmouth Publishing.

Internationella Ekobrottsgruppen (1997). Internationella ekobrott. Ds 1997:51.
Magnusson, Lars (1996). *Sveriges ekonomiska historia*. Rabén Prisma.
Malmsten, Krister (1979). *Datorrelaterade gärningar*. SvJT s.249-282.
Mann, David och Sutton, Mike (1998*). Netcrime. More change in the Organization of Thieving.* Brit. J. Criminol. Vol 38 NO 2 1998.
Martin, D. (1997). *La criminalité informatique*. PUF.
Parker, Donn B. (1998). *Fighting Computer Crime*. John Wiley & Sons.
PM (1997). *Straffprocessuella tvångsmedel och informationsteknik*. Justitiedepartementet.
PM (1998). *Straffrätt och informationsteknik – en grundläggande inventering av lagstiftningsbehovet.* Justitiedepartementet.
PM (1999). *Obervatoriets syn på vissa straff- och processrättsliga lagstiftningsfrågor*. PM från det IT-rättsliga observatoriet. IT-observatoriePM 3:1999.
Rasch, M. D. (1996). *Criminal law and the Internet*. I The Internet and business: A lawyer´s guide to the emerging legal issues. Computer Law Association.
Seipel, Peter. (1990). Begreppet databrott, Nationalencyklopedin, band 4.
SOU (1992). *Information och den nya Informations Teknologin – straff- och processrättsliga frågor m.m.* SOU 1992:110.
SOU (1997). *Bekämpande av penningtvätt*. SOU 1997:36.
RRV (1997). *Datorrelaterade missbruk och brott – en kartläggning gjord av Effektivitetsrevisionen*. RRV 1997:33.
RSV (1999). *Vår omvärld år 2010*. Rapport från Framtidsprojektet, etapp 1. RSV Rapport 1999:3.
Savona, E. U. (1998). *The organisational framework of european crime in the globalisation process.* Transcrime working paper.
Sieber, Ulrich (1998). *Legal aspects of computer-related crime in the information society* – CONCRIME-study. University of Würzburg. Version 1.0, januari 1998.
Solarz, Artur (1981). *Computer Technology and Computer Crime (Aetiological and phenomenological aspects)*. BRÅ Rapport 1981:8.
Solarz, Artur (1983). *Datorteknik och kriminalitet*. Apropå nr 1/83.
Solarz, Artur (1984). *Datorrelaterad brottslighet och rättsväsendets åtgärder*. Apropå nr 6/84.
Solarz, Artur (1985). *Datorteknik och brottslighet*. BRÅ Forskning 1985:3.
Solarz, Artur (1987). *ADB och brott. Kriminalitetens utveckling i ett informationssamhälle*. Publica.
Taloyan, Marina (1999) *Svenska cybernazister och cyberrasister* i *Demokratins förgörare.* Demokratiutredningens skrift nr 28. SOU 1999:10. Stockholm
Telia (1998). *Internet-boven.* Telia, Stockholm.
Ward, Martin (1998). *Barn & Brott av vår tid? Självdeklarerad ungdomsbrottslighet 1971 och 1996.* Licentiatavhandling vid Kriminologiska institutionen, Stockholms universitet.

Westberg, Björn (1998). *Elektronisk handel – varför skatterättsligt intresse?* Svensk skattetidning 2/99.
Ziegler, Jean. (1998). *Les seigneurs du crime. Les nouvelles mafias contre la démocratie.* Points.

English summary

IT-related crime

Published by:
National Council for Crime Prevention (BRÅ)
P.O. Box 1386
SE-111 93 Stockholm
Sweden
Internet: www.brottsforebygganderadet.se

Reference:
BRÅ-report 2000: 2
ISSN 1100-6676, ISBN 91-38-31608-0

Available in Swedish from:
Fritzes Kundtjänst
SE-106 47 Stockholm
Sweden

During the spring, summer and autumn of 1999 the National Council for Crime Prevention (BRÅ) carried out a survey of IT-related crime in Sweden. The questions posed concerned offences, perpetrators, victims, damage caused, threats made and the counter-measures that should be taken.

What are the trends in IT-related crime?

On the basis of the investigation undertaken by the BRÅ among enterprises, administrations, municipalities and county councils with more than 50 employees, it appears that the amount of IT-related crime has increased with 50 per cent since the years 1995 and 1996. This means that every fourth organization has been victimized. During the same period the number of adhesions to public networks such as Internet have almost doubled. At the same time the control and reporting systems of the various organizations have been improved. The marked increase in this kind of crime is probably explained as a combination of increased exposure to risk and a growth in control measures.

The increase in crime has occurred primarily in the private sector. It has been far less noticeable in the public sector.

The most prominent offences and incidents in the survey concern computer viruses, external and internal computer intrusion, the manipulation of data, information theft and fraud.

Virus attacks were the dominant incidents found in the survey. Their number has increased by 47 per cent since the middle of the 1990s. Computer virus attacks constitute a serious, even an extremely serious, threat to the activities of enterprises and administrations.

External and internal computer intrusion is the next largest offence category after computer virus attacks. Computer intrusion was found in the survey to have increased by 48 per cent since the middle of the 1990s. The greatest increase has occurred among private enterprises. With this form of crime the threat posed by employees (insiders) is decidedly more serious than that posed by external persons (outsiders). Despite this, enterprises report far more cases of outsider intrusion to the police than insider intrusion, the respective proportions being 60:40. One reason for this may be that enterprises deal with insider intrusion themselves. They also consider that their reputations may suffer if it becomes known that sensitive IT-crime has occurred. For the years 1997 and 1998 a total of 239 cases of external and internal computer intrusion in the survey were reported to the police.

The manipulation of data and information theft are the forms of crime that enterprises currently do not consider to be especially widespread. Even so, this kind of crime deserves to be taken seriously since it often causes great damage. A firm's information on product development, marketing, contracting, staff, etc. has a significant commercial value. The picture that emerges from the BRÅ survey shows losses involving larger amounts.

Since 1995, manipulation in one form or another has increased by 80 per cent and information theft by 22 per cent. Despite the damage that can be caused, manipulation and information theft is considered in rather more than half of the surveyed enterprises and administrations to be no major threat to their activities. The BRÅ's view is that there is every reason to take these offences seriously.

In the survey, more than half of the IT-incidents reported to the police (329 of 608) during 1997 and 1998 concerned fraud via the Internet. The commonest form was using another person's Internet subscription for free surfing and buying through the Internet using another person's credit card. A considerable increase in reports of fraud via the Internet occurred between 1997 and 1998. The majority of these frauds were reported by private persons.

Other offences reported to the police during 1997 and 1998 included threats and harassments (7), inflicting damage (16) and violations of the law on computerized data and the protection of personal integrity (17).

In the BRÅ survey of private persons having Internet subscriptions, it appeared that one in a hundred had been the subject of a threat or harassment in their e-mail. In addition, five of every hundred private persons had come across child pornography on the net and twelve of every hundred had looked at the national socialist home page.

Perpetrators

It is not easy from the investigations made to arrive at a description of perpetrators. So far as virus attacks and computer intrusions are concerned, the picture that is glimpsed is that most of the offences and incidents are the work of outsiders. When these offences – which are the commonest ones – are excluded, it is insiders (63 per cent) who are responsible for the remaining offences and incidents, for example data manipulation, information theft, etc.

Men dominate in the offences reported to the police; only a few women are named as suspected perpetrators. Men are the ones suspected of computer intrusion. They manipulate, erase and steal programmes, files and data. When women are suspected perpetrators it is for the most part for internal computer intrusion consisting of the unauthorized extraction of information from registers and erasing files, programmes and data. Only three women were suspected of computer fraud. Altogether there were ten women suspects out of a total of 116 suspected perpetrators in the police reports. About 68 per cent of perpetrators were aged 15–25.

Security and damage

Security has been greatly improved over recent years. Thus, for example, the proportion of firms that have preventive protection against external computer intrusion has increased from 40 per cent to just over 65 per cent in the space of a few years. The private sector lags behind the public sector in the prevention of external computer intrusion. Nearly half of all enterprises, administrations, municipalities and county councils lack routines for reporting information theft.

The estimate value of the total damage caused by IT-related crime and misuse amounts to between 37.5 and 194.4 million Swedish crowns (approximately 4.7–24 million US dollars). The average annual cost of damage to a victimized firm is approximately 120,000 Swedish crowns or about 15,000 US dollars.

The criminal justice system

The representatives of majority of firms included in the BRÅ survey considered that they enjoyed good collaboration with criminal justice authorities but thought at the same time that such authorities lacked the capability to investigate and prosecute IT-related crime.

Of the private persons with an Internet subscription only a few thought that police resources were adequate to tackle Internet crime. It was generally considered that the police needed more resources. On the other hand, when the same

group was asked how much crime occurred on the Internet, nearly half responded with amounts varying from small to non-existent.

Key words:
IT-related criminality, IT-related crime, data virus, external and internal computer intrusion, manipulation of data, information theft, Internet fraud, security, damage.